Paul R. Kiesel, State Bar No. 119854
kiesel@kiesel-law.com
Jeffrey A. Koncius, State Bar No. 189803
koncius@kiesel-law.com
Nicole Ramirez, State Bar No. 279017
ramirez@kiesel-law.com
KIESEL LAW LLP
8648 Wilshire Boulevard
Beverly Hills, CA 90211-2910
Tel: 310-854-4444
Fax: 310-854-0812

Stephen M. Gorny [to be admitted *Pro Hac Vice*]
steve@gornylawfirm.com
Chris Dandurand [to be admitted *Pro Hac Vice*]
chris@gornylawfirm.com
THE GORNY LAW FIRM, LC
2 Emanuel Cleaver II Boulevard, Suite 410
Kansas City, MO 64112
Tel.: 816-756-5056
Fax: 816-756-5067

Jay Barnes [to be admitted *Pro Hac Vice*]
jaybarnes5@zoho.com
Rod Chapel [to be admitted *Pro Hac Vice*]
rod.chapel@gmail.com
BARNES & ASSOCIATES
219 East Dunklin Street, Suite A
Jefferson City, MO 65101
Tel.: 573-634-8884
Fax: 573-635-6291

Attorneys for Plaintiffs

(Additional Attorneys Listed on Signature Page)

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

WINSTON SMITH; JANE DOE I; and JANE DOE II, on behalf of themselves and all others similarly situated,

Plaintiffs,

v.

FACEBOOK, INC.; AMERICAN CANCER SOCIETY, INC.; AMERICAN SOCIETY OF CLINICAL ONCOLOGY, INC.; MELANOMA RESEARCH FOUNDATION; ADVENTIST HEALTH SYSTEM; BJC HEALTHCARE; CLEVELAND CLINIC; and UNIVERSITY OF TEXAS - MD ANDERSON CANCER CENTER,

Defendants.

CASE NO.

CLASS ACTION

COMPLAINT

JURY TRIAL DEMANDED

TABLE OF CONTENTS

EXHIBITS TO COMPLAINT

Exhibit A -	Facebook Terms
Exhibit B -	Facebook's Data Policies
Exhibit C -	Facebook's "Cookie Use" page
Exhibit D -	Facebook's Developer pages
Exhibit E -	A partial chart of medical category interest lists for sale for directing marketing of Facebook users in the United States
Exhibit F -	ACS's Privacy Policy
Exhibit G -	ASCO's Privacy Policy
Exhibit H -	MRF's Privacy Policy
Exhibit I -	ShawneeMission.org Privacy Policy
Exhibit J -	BJC's Privacy Policy

I. OVERVIEW

1. This class action complaint seeks damages and injunctive relief for privacy violations by Facebook on the websites Cancer.org, Cancer.net, Melanoma.org, ShawneeMission.org, BarnesJewish.org, ClevelandClinic.org, MDAnderson.org, and other health care and hospital websites (hereafter, the "health care Defendants").

2. Plaintiffs' cancer and other sensitive health-related Internet communications with these medical websites were divulged to Facebook and acquired by Facebook along with the Plaintiffs' personally-identifiable information. In addition, Facebook acquired, tracked, and used the Plaintiffs' sensitive medical information collected through medical websites and the Facebook website for purposes of direct marketing.

3. The disclosures, tracking, and use of their sensitive medical information for direct marketing were all done without Plaintiffs' knowledge or consent in violation of their privacy rights under federal and state law.

4. Defendant Facebook failed to disclose to its users that it (a) tracks, intercepts, and acquires user communications in violation of other websites' privacy policies, (b) tracks, intercepts, and acquires user communications with medical websites, including the websites of medical providers subject to HIPAA and other medical privacy laws, and (c) uses the personal information it gathers from its users, including sensitive medical information, to place its users into medical categories for purposes of direct marketing.

5. The health care Defendants' actions in divulging sensitive personally-identifiable medical information about the Plaintiffs to Facebook without the Plaintiffs' knowledge or consent violated the Privacy Policies at each website at issue in this case. However, Plaintiffs are without knowledge as to whether the disclosures by the health care Defendants were willful and knowing because Facebook does not publicly disclose the full extent of its tracking to either its users or website developers.

II. PARTIES

6. Plaintiff Winston Smith is a resident of Missouri and a registered Facebook user.[1]

7. Plaintiff Jane Doe is a resident of Kansas and a registered Facebook user.

8. Plaintiff Jane Doe II is a resident of Missouri and registered Facebook user.

9. Defendant Facebook, Inc. ("Facebook") is a publicly traded Delaware corporation headquartered at 156 University Avenue, Palo Alto, California 94301. Facebook does business throughout the United States and the world, deriving substantial revenue from interstate commerce.

10. Defendant American Cancer Society, Inc. ("ACS") is a not-for profit corporation headquartered at 250 Williams Street, NW, Atlanta, Georgia 30303. ACS does business throughout the United States, deriving substantial revenue from interstate commerce.

11. Defendant American Society of Clinical Oncology, Inc. ("ASCO") is a not-for-profit corporation headquartered at 2318 Mill Road, No. 800, Alexandria, Virginia 22314. ASCO does business throughout the United States, deriving substantial revenue from interstate commerce.

12. Defendant Melanoma Research Foundation ("MRF") is a 501(c)(3) non-profit organization headquartered at 1411 K Street NW, Ste. 800, Washington, D.C. 20005. MRF does business throughout the United States, deriving substantial revenue from interstate commerce.

13. Defendant Adventist Health System ("Adventist") is a non-profit health care system operating 44 hospitals across the United States headquartered at 900 Hope Way, Altamonte Springs, Florida 32714. Adventist does business throughout the United States, deriving substantial revenues from interstate commerce.

14. Defendant BJC Healthcare ("BJC") is a non-profit health care provider based in St. Louis, Missouri headquartered at One Barnes-Jewish Hospital Plaza, St. Louis, Missouri 63110. BJC does business throughout the United States, deriving substantial revenue from interstate

[1] This Complaint reveals personal medical information about the Plaintiffs which were wrongfully intercepted, disclosed, and shared amongst the Defendants. Plaintiffs file this Complaint listed anonymously to protect their medical information from further disclosure.

commerce.

15. Defendant Cleveland Clinic ("Cleveland Clinic") is a non-profit health care provider headquartered at 9500 Euclid Avenue, Cleveland, Ohio 44195. Cleveland Clinic does business throughout the United States, deriving substantial revenue from interstate commerce.

16. Defendant University of Texas – MD Anderson Cancer Center ("MD Anderson") is a non-profit health care provider headquartered at 1515 Holcombe Boulevard, Houston, Texas 77030. MD Anderson does business throughout the United States, deriving substantial revenue from interstate commerce.

III. JURISDICTION AND VENUE

17. This Court has personal jurisdiction over the Defendants because each has sufficient minimum contacts with this district in that they operate and market their websites throughout the country and in this district. Additionally, Defendant Facebook is headquartered in this district.

18. This Court has subject matter jurisdiction pursuant to 28 U.S.C. §1331 because this action arises under 18 U.S.C. §2510, et. seq., (the Electronic Communications Privacy Act). This Court further has subject matter jurisdiction pursuant to 28 U.S.C. §1332(d) (the Class Action Fairness Act) because the amount in controversy exceeds $5,000,000, exclusive of interest and costs, and a member of the class is a citizen of a State different from any Defendant.

19. This Court has supplemental jurisdiction over the remaining state law claims pursuant to 28 U.S.C. §1367 because the state law claims form part of the same case or controversy under Article III of the United States Constitution.

20. Venue is proper in this district because a substantial part of the events or omissions giving rise to the claim occurred in this judicial district and because Facebook's Terms of Use governing its relationship with its users and developers adopt California law and choose California as the venue for disputes.

IV. FACTS COMMON TO ALL COUNTS

A. How the Internet Works

21. Internet users employ web-browsers to send and receive electronic

communications.

22. Web-browsers are software applications that allow consumers to send, receive, and view electronic communications on the Internet. Web browsers include a Terms of Use or Service, which prohibit users from engaging in unlawful or unauthorized tracking of the communications of others or from using the service to engage in criminal or otherwise unlawful acts. For example, major web-browsers such as Google Chrome, Microsoft Internet Explorer, and Apple Safari all expressly prohibit unlawful acts, and Plaintiffs are not aware of any major web-browser which consents to the use of its service for criminal or otherwise unlawful acts.

23. The most popular web-browsers include Apple Safari, Microsoft Internet Explorer, Google Chrome, and Mozilla Firefox.

24. Every website is hosted by a computer server through which it sends and receives communications with Internet users via their web-browsers to display web-pages on users' monitors and screens, depending upon the user's chosen computing device.

25. The basic command web-browsers use to communicate with website servers is called the 'GET command' or 'GET request.' For example, when an Internet user types "www.cancer.org" into the navigation bar of their web-browser and hits 'Enter' (or, more commonly, when an Internet user clicks on a hyper-link), the user's browser sends a GET request to the server for Cancer.org. This GET request instructs the Cancer.org server to send the information contained on the Cancer.org homepage to the user's web-browser for display.

26. Another basic command is the 'POST' command, which is used when a user enters data into a form on a website and clicks 'Enter' or the submit button. The POST command sends the data entered into the form to the website.

27. Each website server has an Internet Protocol Address ("IP address"). For example, the IP address for the website www.cancer.org is "69.20.25.160." An IP address, however, is not the same thing as a Uniform Resource Locator, or more commonly, URL. In this case, Cancer.org has just a single or a handful of IP addresses for all of the articles, essays, and other communications hosted on its web-server. Thus, revealing that an Internet user sent a series of communications to 69.20.25.160 only reveals the parties to the communication – the user and the

American Cancer Society. In contrast, a full-string detailed URL (as explained below) reveals both the parties to the communication and its content.

28. A URL is composed of several different parts.[2] For example, consider the following URL:

http://www.cancer.org/cancer/testicularcancer/moreinformation/doihavetesticularcancer/do-i-have-testicular-cancer-intro

a. **http://**: This is the protocol identified by the web browser to the web server which sets the basic language of the interaction between browser and server. The back-slashes indicate that the browser is attempting to make contact with the server;

b. **www.cancer.org**: This is the name that identifies the website and corresponding web server, with which the Internet user has initiated a communication;

c. **/cancer/**: This part of the URL indicates a folder on the web server, a part of which the Internet user has requested;

d. **/testicularcancer/moreinformation/doihavetesticularcancer**: This part of the URL indicates a sub-folder on the web-server, a part of which the Internet user has requested;

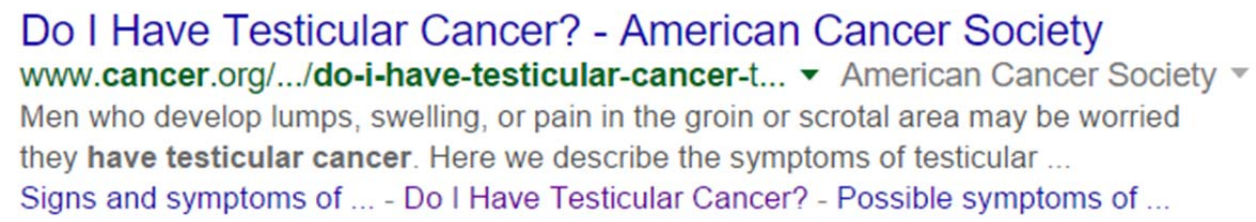
e. **/do-i-have-testicular-cancer-intro/:** This part of the URL is the file name for the particular file containing the information the Internet user has requested;

f. **cancer/testicularcancer/moreinformation/doihavetesticularcancer/do-i-have-testicular-cancer-intro:** This combination of the folder, sub-folder, and exact file name is called the "file path".

29. To further illustrate the distinction between an IP address and a full-string detailed URL, consider an Internet user seeking information on testicular cancer. The user might type the

[2] Microsoft.com, URL Path Length Restrictions (Sharepoint Server 2010), http://technet.microsoft.com/en-us/library/ff919564(v=office.14).aspx.

exact search term, "Do I Have Testicular Cancer?" into a search engine, and one result they would get is a link to the article at Cancer.org:



The user who clicks on the link "Do I Have Testicular Cancer?" would send a communication through the user's browser to the American Cancer Society seeking that information via a detailed GET request and the full-string detailed URL: http://www.cancer.org/cancer/testicularcancer/moreinformation/doihavetesticularcancer/do-i-have-testicular-cancer-intro. The IP address for the American Cancer Society's website would be the same whether the user (a) went to the home page at Cancer.org or (b) sent this detailed request for information via GET request and URL. When the user clicked on the link "Do I Have Testicular Cancer?", they would receive in return an essay from the American Cancer Society on testicular cancer and its diagnosis.

30. Although a single webpage appears on a user's screen as a complete product, it is, in reality, an assembled collage of independent parts. Each different part of a webpage – i.e. the text, pictures, advertisements, sign-in box and other parts – often exist on different servers, which are many times operated by separate companies.

31. To display each part of a single webpage as one complete product, the host server for the webpage leaves parts of the page blank to be filled in by third parties.

32. Upon receiving a GET request from a user's web-browser, the website server of the recipient (in this case Cancer.org) contemporaneously re-directs the user's web-browser to send a separate but simultaneous GET command through a separate channel to the third-party responsible for filling out a portion of the page it previously left blank.

33. In addition to the GET command received by the third-party, the detailed URL from the first domain is also often acquired by the third-party. These URLs are called 'referer' headers.

34. The contemporaneous re-direction and acquisition by the third-party through a separate path is accomplished through each individual Internet user's web-browser without any further action or knowledge of the user.

35. For example, on the Cancer.org homepage provided above, the user sends a GET request from his browser to Cancer.org by typing the page address into his web-browser or by clicking on a link to go to that page. Unbeknownst to the user sending the communication, Cancer.org includes Facebook code. Upon Cancer.org receiving the GET request, Facebook's code directs Cancer.org to contemporaneously commandeer the user's web-browser for Facebook's own purposes, ultimately commanding the user's browser to send a separate but simultaneous GET request through a different channel to Facebook's server that is attached to an exact duplicate of the user's communication to Cancer.org, in order to fill out the small piece of the Cancer.org webpage associated with Facebook.

36. Without the knowledge, consent, or any action of the user, the entire process happens in milliseconds, with the precise length of time from original GET request to complete fulfillment determined by the user's Internet speed and the speed of the website server and server(s) to which the user's referer URL and GET requests were contemporaneously re-directed through separate channels. The third-parties acquire the communications before the website's full response is visible on the user's web-browser.

37. Many parts of the page left blank and hosted by other servers are not necessary for websites to function, including, in this example from Cancer.org, the part relating to Facebook.

38. Referer headers that include the full-string URL or content contained within the GET request to the first-party website also are not necessary. Facebook has long understood this and also that referer headers often include sensitive content. In 2010, on a Facebook blog, Facebook engineer Matt Jones explained:

> [S]ometimes referrers just don't belong – maybe there is sensitive information in a URL, or maybe a site just doesn't wants its users' browsers telling others how they use the site. … Facebook is one site where referrers don't belong. As part of our continued efforts to protect users' privacy, we proactively protect our users from exposing how they navigated to an external site. To this end, we have designed a redirector …

[which] remove[s] the referrer of the page on which the user clicked.

See "Protecting Privacy with Referrers" by Matt Jones, May 24, 2010, available by sending the following communication in a web-browser: https://www.facebook.com/notes/facebook-engineering/protecting-privacy-with-referrers/392382738919/.

39. As explained in more detail below, it is through similar processes that the health care Defendants disclose (whether purposeful or not) and through which Facebook acquires the Plaintiffs' sensitive personally-identifiable medical communications without the Plaintiffs' knowledge or consent and in violation of state and federal laws, the health care Defendants' various privacy policies, and Facebook's duty of good faith and fair dealing with its users.

B. The Birth of Internet "Cookies"

40. In the Internet's formative years, advertising on websites followed the same model as traditional newspapers. Just as a sporting goods store would choose to advertise in the sports section of a traditional newspaper, advertisers on the early Internet paid for ads to be placed on specific web pages based on the type of content displayed on the web page.

41. Computer programmers eventually developed "cookies" – small text files that web-servers can place on a person's web-browser and computing device when that person's web-browser interacts with the website server. Cookies can perform different functions. Eventually, some cookies were designed to track and record an individual Internet user's communications with and activities on websites across the Internet.

42. In general, cookies are categorized by (1) duration, and (2) party.

a. Cookie Classifications by "Duration"

i. "Session cookies" are placed on a person's computing device only for the time period during which the user is navigating the website that placed the cookie. The person's web-browser normally deletes session cookies when the user closes the browser.

ii. "Persistent cookies" are designed to survive beyond a single Internet-browsing session. The party creating the persistent cookie determines its lifespan. As a result, a persistent cookie can record a

person's Internet browsing history and Internet communications for years. By virtue of their lifespan, persistent cookies can track a person's communications with and activities on dozens or hundreds of websites on the Internet. Persistent cookies are also sometimes called "tracking cookies."

b. Cookie Classifications by "Party"

i. "First-party cookies" are set on a user's device by the website the user intends to visit. For example, Cancer.org sets a collection of its own cookies on user's browsers when they visit any webpage on Cancer.org. First-party cookies can be helpful to the user, server, and/or website to assist with security, log-in, and functionality.

ii. "Third-party cookies" are set by website servers other than the website or server the user intends to visit. For example, the same user who visits Cancer.org will also have cookies placed on their device by third-party web-servers, including Facebook. Unlike first-party cookies, third-party cookies are not typically helpful to the user. Instead, third-party cookies typically work in furtherance of data collection, behavioral profiling, and targeted advertising.

43. Enterprising online data companies, such as Facebook, soon developed methods to monetize and profit from cookies. Specifically, third-party persistent tracking cookies are used to sell advertising that is customized based upon a particular person's Internet communications and browsing habits. To build an individual profile of Internet users, data companies like Facebook assign each specific user a unique, or a set of unique, numeric or alphanumeric identifiers that are associated with specific cookies Facebook has assigned to each of its users. Facebook users pay for Facebook's services with their personal information. Facebook's users exchange something of value – access to their personal information – for Facebook's services and Facebook's promise to safeguard that personal information and to act in a manner that is reasonable, consistent with the spirit of the bargain made, and does not abuse Facebook's power to specify the terms of the

contract.[3]

44. Even where they do not allow advertisements, website owners often allow third-party data-tracking companies to track users of their websites.

45. When allowing third-party companies to track users and/or place advertisements on their website, the host website provides the third-party access to communications it receives from and sends to users. As described above, upon receiving a GET request from an Internet user's web-browser, the website's server will, unbeknownst to that individual user, immediately and contemporaneously re-direct the user's browser to send a GET request to the third-party company, who then uses the information to create detailed profiles of users. When a user has a third-party cookie present on their web-browser, the third-party will be able to connect the communication to a particular user.

46. In many cases, the third-party receives the re-directed GET request and a copy of the user's communication to the first-party website before the first-party website's response to the user's communication appears on the user's screen. The re-directed communication from the user includes a referrer header which identifies information about both the user's communication and the website's response in the form of a URL.

47. The transmission of such information is contemporaneous to the user's communication with the first-party website. However, because of "packet-switching" technology, it also occurs while the information is in storage by the first-party website as well as the user's web-browser, ISP and personal computing device.

48. The entire process occurs within milliseconds and the web page appears on the Internet user's browser as one complete product, without the person ever knowing that multiple GET requests were executed by the browser at the direction of the web site server, and that first-party and third-party cookies were placed and accessed in the user's web-browser. Indeed, the user has only made one knowing and purposeful communication – a GET request to the website with

[3] However, as set forth herein, Facebook's conduct evades the spirit of the bargain made between Facebook and its users because Plaintiffs and the class members did not receive the benefit of the bargain for which they contracted and for which they paid valuable consideration in the form of their personal information which has ascertainable value to be proven at trial.

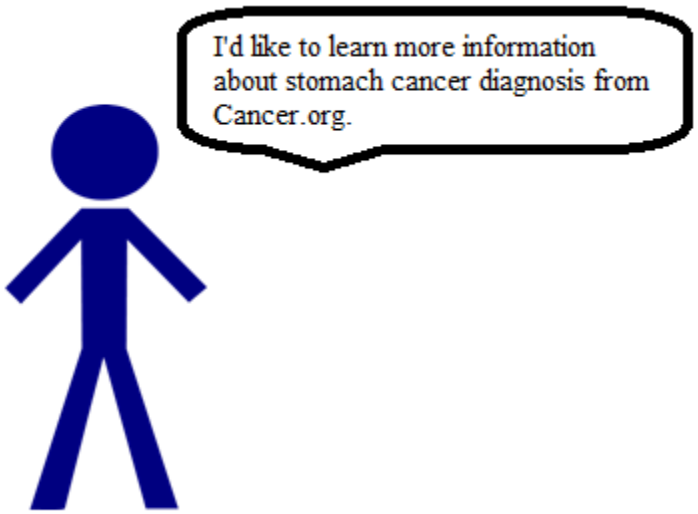
which they intended to send and receive communications, such as Cancer.org.

C. Illustrating How Internet Communications Happen

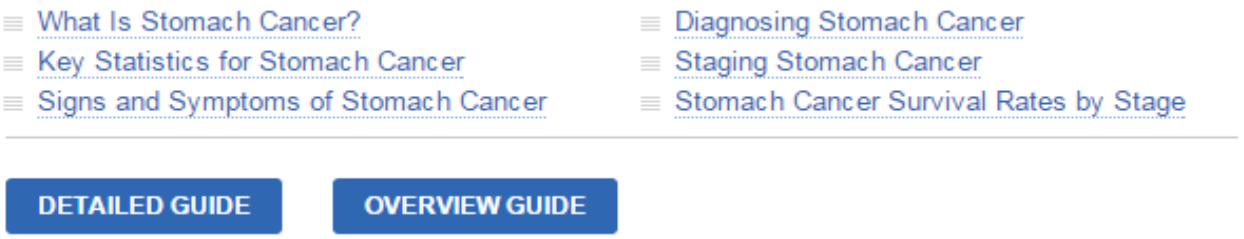
49. As described above, an Internet communication consists of several separate but simultaneous communications and signals.

50. The following illustrates the flow of information that would occur for a user sending and receiving communications from the American Cancer Society via Cancer.org relating to stomach cancer diagnosis:

a. The communication between the user and Cancer.org starts when the user decides to seek information on the relevant topic from the American Cancer Society.

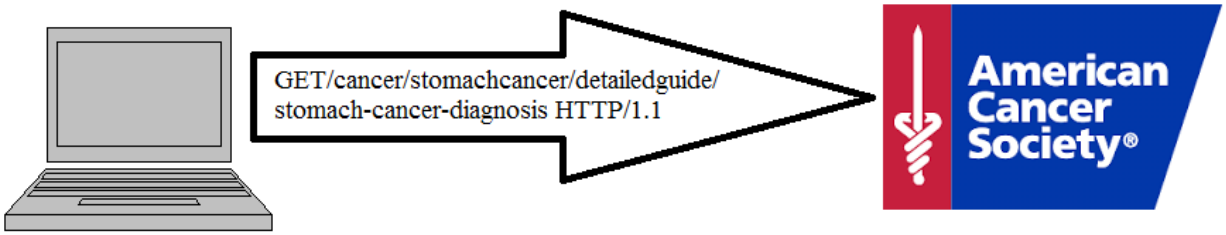


b. The user can send the communication via one of two methods. The user can either type – www.cancer.org/cancer/stomachcancer/detailedguide/stomach-cancer-diagnosis into their toolbar, or the user can click on a link. For the communication above, the link "Diagnosis Stomach Cancer" illustrated below would send the user to the Cancer.org page for Stomach Cancer Diagnosis. This screenshot comes from the webpage: http://www.cancer.org/cancer/stomachcancer/index.



c. Whether the user manually types the URL into their toolbar or uses the technological shortcut of clicking on their mouse, the intent and the effect is the same: the user has sent a communication to Cancer.org seeking information about "stomach cancer diagnosis."

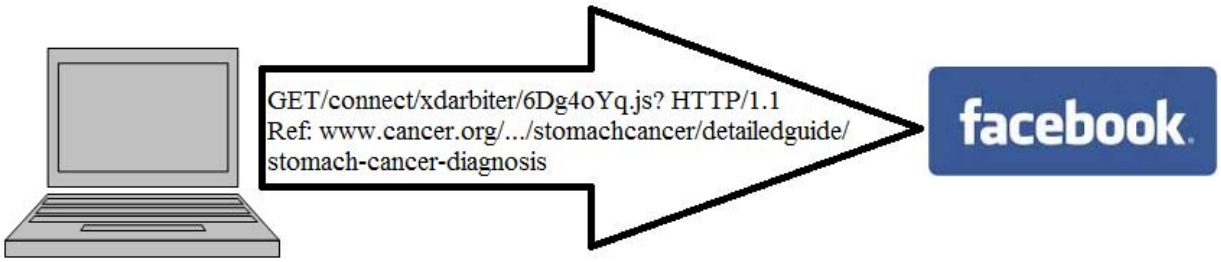
d. Immediately upon the user hitting enter or clicking on their mouse, their web-browser sends a 'GET' request to the American Cancer Society's web-server requesting the relevant information.



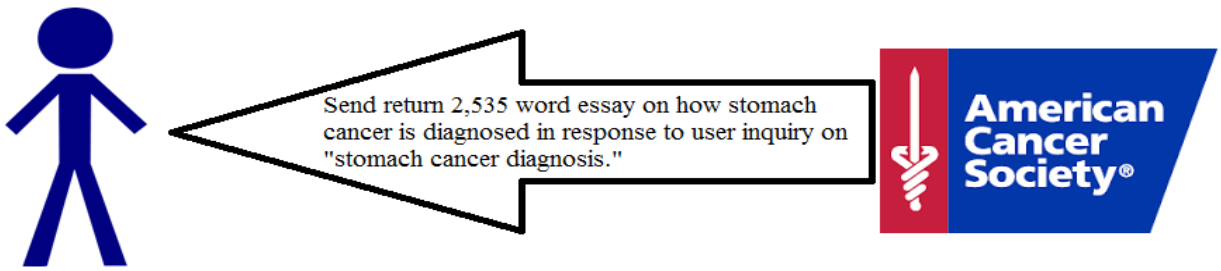
e. Unbeknownst to the user sending the communication, the American Cancer Society webpage includes Facebook code, that upon ACS receiving the GET request, Facebook's code directs the American Cancer Society's web-server to, in turn, commander the user's web-browser for Facebook's own purposes, ultimately commanding the user's browser to send a separate but simultaneous 'GET' request to Facebook that is attached to an exact duplicate of the user's communication to the American Cancer Society.

f. Without the knowledge, consent, or any action of the user, the user's web-browser follows the commands received as a result of Facebook's computer

code by sending a 'GET' request to Facebook's server. This GET request, however, is not identical to the request sent to the American Cancer Society. However, it is accompanied by a 'referer header' that includes the detailed URL which contains within it an exact copy of the GET request that the user sent to the American Cancer Society's web-server – as well as information relating to the substance, purport, or meaning of the user's intended communication – i.e. "stomach cancer diagnosis." In addition to acquiring these two pieces of information, Facebook also accesses cookies located on the user's computer that personally identify the user to Facebook. Through this process, Facebook has acquired knowledge that the user is seeking information on stomach cancer diagnosis – attached to personally-identifying information. Facebook acquires all of this information before the communications between the user and the American Cancer Society is completed.



g. The American Cancer Society responds to the user's request for information on stomach cancer diagnosis by sending a 2,535 word essay on, not surprisingly, how stomach cancer is diagnosed. Like the user's original action seeking information on stomach cancer diagnosis (whether by typing it into the toolbar or clicking a hyper-link), the American Cancer Society essay response involves sentient thought by a human being. It is more than mere computer code directing software or hardware to take an action.



51. Significantly, Facebook is not a party to the user's GET request to the American Cancer Society for a "detailed guide" on "stomach cancer diagnosis." Nor is Facebook a party to the American Cancer Society's 2,535 essay response to the user providing a "detailed guide" on "stomach cancer diagnosis."

52. In effect, Facebook's code operates as an automatic routing program that commandeers the browsers of Internet users sending and receiving communications with medical websites, causing those browsers to send exact duplicates of each user's private communications with those medical websites to Facebook in the middle of the communication between the user and the medical website without the knowledge, consent, or any other action of the Internet user.

D. The Value of the Personal Information Defendants Collect

53. To data companies, cookies and the corresponding targeted ads they enable provide an unprecedented opportunity to reach potential consumers. The value of the information that data companies like Facebook take from people who use the Internet is well understood in the e-commerce industry. Personal information is now viewed as a form of currency. Professor Paul M. Schwartz noted in the Harvard Law Review:

> Personal information is an important currency in the new millennium. The monetary value of personal data is large and still growing, and corporate America is moving quickly to profit from the trend. Companies view this information as a corporate asset and have invested heavily in software that facilitates the collection of consumer information.[4]

54. Likewise, in the Wall Street Journal, privacy expert and fellow at the Open Society Institute, Christopher Soghoian, noted:

[4] Paul M. Schwartz, Property, Privacy, and Personal Data, 117 Harv. L. Rev. 2055, 2056-57 (2004).

> The dirty secret of the Web is that the "free" content and services that consumers enjoy come with a hidden price: their own private data. Many of the major online advertising companies are not interested in the data that we knowingly and willingly share. Instead, these parasitic firms covertly track our web-browsing activities, search behavior and geolocation information. Once collected, this mountain of data is analyzed to build digital dossiers on millions of consumers, in some cases identifying us by name, gender, age as well as the medical conditions and political issues we have researched online. Although we now regularly trade our most private information for access to social-networking sites and free content, the terms of this exchange were never clearly communicated to consumers.[5]

55. In the behavioral advertising market, "the more information is known about a consumer, the more a company will pay to deliver a precisely-targeted advertisement to him."[6]

56. In general, behaviorally targeted advertisements based on a user's tracked Internet activity sell for at least *twice* as much as non-targeted, run-of-network ads,[7] produce 670 percent more clicks on ads per impression than run-of-network ads, and are more than twice as likely to convert users into buyers of an advertised product as compared to run-of-network ads.[8]

57. The cash value of users' personal information, including medical information, can be quantified. In a recent study, researchers determined the value that American Internet users place on their "health condition" is second only to "Passwords (login details)":[9]

---

[5] Julia Angwin, *How Much Should People Worry About the Loss of Online Privacy?*, THE WALL STREET JOURNAL (Nov. 15, 2011).

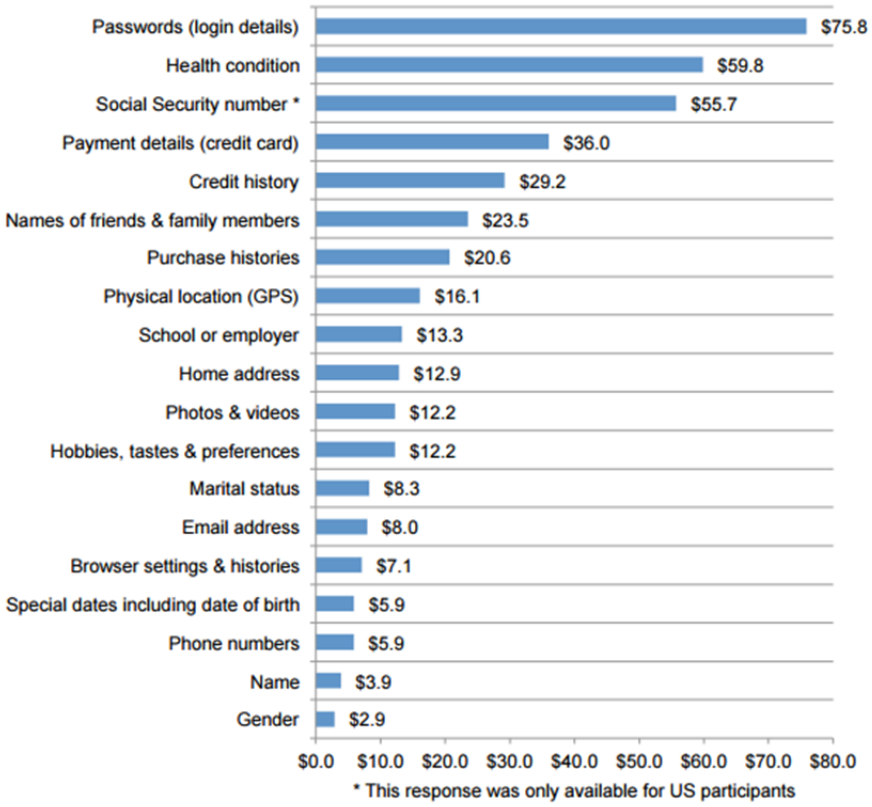
[6] http://www.ftc.gov/os/2010/12/101201privacyreport.pdf at 37.

[7] NetworkAdvertising.org, Study Finds Behaviorally-Targeted Ads More Than Twice As Valuable, Twice As Effective As Non-Targeted Online Ads, http://www.networkadvertising.org/pdfs/NAI_Beales_Release.pdf

[8] Howard Beales, *The Value of Behavioral Advertising*, 2010. http://www.networkadvertising.org/pdfs/Beales_NAI_Study.pdf

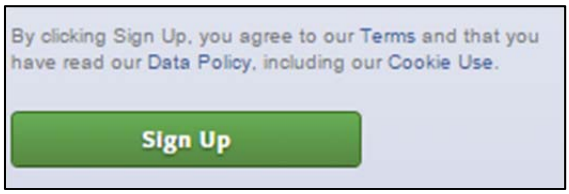
[9] Ponemon Institute, Privacy and Security in a Connected Life: A Study of US, European and Japanese Consumers, March 2015.

Figure 17. How much is your personal data worth?
Extrapolated average value = $19.60
n = 1,078



E. Facebook's Data / Privacy Policy, Internet Tracking, and Business Model

58. On sign-up, Facebook requires users to click a green Sign Up button:



59. Facebook's Terms, Data Policy, and Cookie Use (each highlighted in blue above) acknowledgements link to provisions of a browse-wrap contract. However, because the disclaimer is placed directly above the Sign-Up button it has a click-wrap quality and constitutes a valid contract.

60. Facebook's Terms are contained in a document called the "Statement of Rights and Responsibilities," which has two paragraphs relating to privacy. The first such paragraph states:

> Your privacy is very important to us. We designed our Data Policy to make important disclosures about how you can use Facebook to share with others and how we collect and can use your content and information. We

> encourage you to read the Data Policy, and to use it to help you make informed decisions.

See Exhibit A for a copy of Facebook Terms.

61. The next reference to privacy is at the end of the Terms document. It states:

> By using or accessing Facebook services, you agree that we can collect and use such content and information in accordance with the Data Policy as amended from time to time.

62. Facebook Data Policy page to which users are sent via the link above vaguely discloses to users that it collects information about their Internet use on third-party websites:

> **Information from websites and apps that use our Services.**
> We collect information when you visit or use third-party websites and apps that use our Services (like when they offer our Like button or Facebook Log In or use our measurement and advertising services). This includes information about the websites and apps you visit, your use of our Services on those websites and apps, as well as information the developer or publisher of the app or website provides to you or us.

> **Information from third-party partners.**
> We receive information about you and your activities on and off Facebook from third-party partners, such as information from a partner when we jointly offer services or from an advertiser about your experiences or interactions with them.

63. Facebook purports to have two data policies. One is the web-page to which users are sent via the link at sign-up. A second "Full Data Policy" is provided on another page. *See* Exhibit B for copies of both of Facebook's Data Policies.

64. To the extent to which there are differences in Facebook's two data policies, the Data Policy to which Facebook provides a link to users at sign-up is the only valid policy for legal purposes.

65. Facebook's Data Policies fail to disclose that it tracks, collects, and intercepts sensitive medical information and communications of its users.

66. Facebook's Data Policies fail to disclose that it tracks, collects, and intercepts users' communications with the websites of medical providers or other health care websites.

67. Facebook's Data Policies fail to disclose that it tracks, collects, and intercepts users' communications in violation of the privacy policies at other websites.

68. Facebook's Data Policies fail to disclose that it tracks, collects, and intercepts users' communications in violation of laws designed to protect the privacy of sensitive health information including, but not limited to, the Health Insurance Portability and Accountability Act of 1996, 42 U.S.C. § 1320d, et seq. ("HIPAA").

69. Facebook's Data Policies fail to disclose that it collects directly from Plaintiffs' web-browsers individually-identifiable information about the users' medical history and condition.

70. Facebook's Data Policies fail to disclose that it uses the Plaintiffs' sensitive medical information for direct marketing purposes, placing users into tranches of medically-sensitive categories for sale to advertisers.

71. Facebook's "Cookie Use" page informs users that it uses cookies to individually target users with advertising:

Advertising, insights and measurement	Things like Cookies and similar technologies (such as information about your device or a pixel on a website) are used to understand and deliver ads, make them more relevant to you, and analyze products and services and the use of those products and services. For example, we use cookies so we, or our affiliates and partners, can serve you ads that may be interesting to you on Facebook Services or other websites and mobile applications. We may also use a cookie to learn whether someone who was served an ad on Facebook Services later makes a purchase on the advertiser's site or installs the advertised app. Similarly, our partners may use a cookie or another similar technology to determine whether we've served an ad and how it performed or provide us with information about how you interact with them. We also may work with an advertiser or its marketing partners to serve you an ad on or off Facebook Services, such as after you've visited the advertiser's site or app, or show you an ad based on the websites you visit or the apps you use – all across the Internet and mobile ecosystem. We also may use Cookies to provide advertisers with insights about the people who see and interact with their ads, visit their websites, and use their apps. Learn more about the information we receive, how we decide which ads to show you on and off Facebook Services, and the controls available to you.

See Exhibit C for a copy of the "Cookie Use" page.

72. The relationship between Facebook and its users is governed by the documents to

which it provides users with links at sign-up: its Terms, Data Policy, and Cookie Use web-pages.

73. Facebook's Terms page includes links at the bottom to pages which either do not apply to ordinary users or which do not make any disclosure relating to its Social Plugins, which allow Facebook users to push, for example, a "Like" button which Facebook explains lets "people share pages and content from your site back to their Facebook profile with one click, so all their friends can read them." These pages include: Payment Terms, Platform Page, Facebook Platform Policies, Advertising Policies, Self-Serve Ad Terms, Promotions Guidelines, Facebook Brand Resources, How to Report Claims of Intellectual Property Infringement, Pages Terms, and Community Standards, respectively.

74. Separate from the pages and documents to which Facebook provides users with a link at sign-up, it also maintains a "Help" page for "Social Plugins" in which it provides the following:[10]

> **What information does Facebook get when I visit a site with the Like button?**
>
> If you're logged into Facebook and visit a website with the **Like** button, your browser sends us information about your visit. Since the **Like** button is a little piece of Facebook embedded on another website, the browser is sending info about the request to load Facebook content on that page.
>
> We record some of this info to help show you a personalized experience on that site and to improve our products. For example, when you go to a website with a **Like** button, we need to know who you are in order to show you what your Facebook friends have liked on that site. The data we receive includes your user ID, the website you're visiting, the date and time and other browser-related info.
>
> If you're logged out or don't have a Facebook account and visit a website with the **Like** button or another social plugin, your browser sends us a more limited set of info. For example, because you're not logged into Facebook, you'll have fewer cookies than someone who's logged in. Like other sites on the Internet, we receive info about the web page you're visiting, the date and time and other browser-related info. We record this info to help us improve our products.
>
> As our Data Policy indicates, we use cookies to show you ads on and off Facebook. We may also use the info we receive when you visit a site with social plugins to help us show you more interesting and useful ads.

[10] See https://www.facebook.com/help/443483272359009/.

75. The Facebook "Like" button disclosure above is not contained within the Terms, Data Policy, or Cookie Use pages to which Facebook provides a link to users at sign-up.

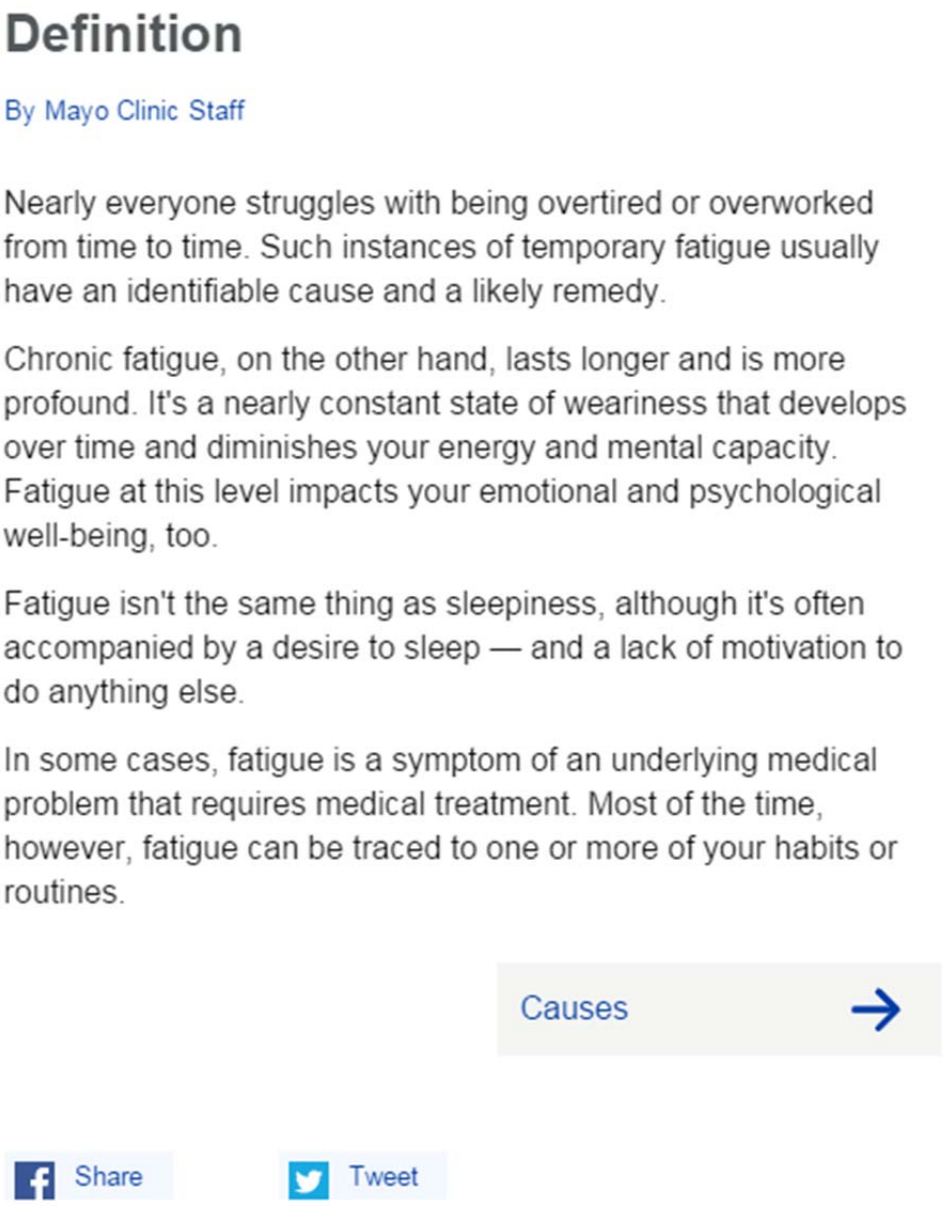
76. Plaintiffs are not aware of any direct link contained within the sign-up disclosures to the information contained on the Help page for "What information does Facebook get when I visit a site with the Like button?"

77. Plaintiffs are not aware of any rational or likely way that a Facebook user might find or be informed of the "What information does Facebook get when I visit a site with the Like button?" page through the Terms, Data Policy, and Cookie Use pages. Instead, the only methods of which Plaintiffs are aware would be if a user did a specific search for the information on the Facebook website, or through the successful completion of a Byzantine maze: from the "Cookie Use" link, the user could click on one of the 18 links on the left-hand portion of the page to which there are no references in the body of the "Cookie Use" disclosure. Those 18 links on the "Cookie Use" page include over 304 sub-links. If the user clicked the "Apps, Games, & Payments" link on the left-hand column of the "Cookie Use" page, they would be shown a sub-menu with 10 links. Of those 10 sub-menu links, there are another 19 sub-links. To reach the relevant page, a user would have to click on "About Social Plugins," the second-to-last of the 10 sub-menu links. The user still would not be finished, but instead would be presented with three further links: "What are social plugins?", "How do social plugins work?" and "What information does Facebook get when I visit a site with the Like button?" Finally, if the user clicked on the link, they would be presented with the disclosure.

78. Facebook does not disclose that it may track and intercept communications on webpages that do not have a "Like" button or a designated "Share" button, but instead only a Facebook icon. In fact, however, Facebook does track users on pages lacking a Like button.

79. **Facebook Tracking Does Not Occur on Most Medical Websites** – Facebook, however, does not track or intercept user communications with every website on which the Facebook icon appears. For example, the websites for the Mayo Clinic (mayoclinic.org) and Johns Hopkins Medicine (hopkinsmedicine.org) include a small Facebook icon on nearly every page, but do not permit Facebook to track user communications. The same is true for hundreds if not

thousands of other medical websites. This screen shot from the Mayo Clinic webpage, http://www.mayoclinic.org/symptoms/fatigue/basics/definition/sym-20050894, illustrates the point. Mayo Clinic does not disclose and Facebook does not track or intercept user communications on this webpage despite the fact that a Facebook "Share" icon appears on it:



80. Facebook earns revenue primarily through targeted advertising based on digital dossiers Facebook builds on each of its users from tracking those users' communications across the Internet. In 2014, Facebook earned nearly $11.5 billion from advertising.

81. As Facebook has explained in its annual report:

> We generate the substantial majority of our revenue from selling advertising placements to marketers. Our ads let marketers reach people on Facebook based on a variety of factors including age, gender, location, and interests. Marketers purchase ads that can appear in multiple places including in News Feed on mobile devices and personal computers, and on the right-hand side of personal computers.
>
> Our ad planning tools are designed to align with marketers' business goals. When marketers create an ad campaign on Facebook, they can specify their budget, marketing objectives and the types of people they want to reach. Facebook's ad serving technology then dynamically determines the best available ad to show each person based on those dimensions.[11]

82. Facebook's digital profiles are built primarily through the use of cookies and other tracking technologies. In particular, Facebook tracks users with the following cookies:

a. The 'c_user' cookie is the Facebook equivalent of a Social Security number. It is persistent and unique to each individual Facebook user.

b. The 'datr' cookie is used by Facebook to individually identify each web-browser used to access Facebook. It is persistent and unique to each individual browser that accesses Facebook. In many cases, there is only one 'c_user' cookie associated with a 'datr' cookie. This is true for those Facebook users who are the exclusive users of their personal computers. In other cases, there are only a very few 'c_user' cookies associated with each 'datr' cookie. For example, a computer shared by a family with multiple Facebook users will have multiple c_user cookies associated with the 'datr' cookie. Finally, public computers may have several unrelated c_user cookies associated with a datr cookie. In 2015, Facebook began allowing users to download portions of their Facebook data, including the last four digits of 'datr' cookies Facebook associates with their user account. Facebook's data download process providing users with information on the

[11] Facebook 2014 Annual Report (SEC Form 10-K) at 5. – available at: http://files.shareholder.com/downloads/AMDA-NJ5DZ/1372113521x0x852173/F61276C5-0AE9-49DE-BFD9-087398F85EC8/FB2014AR.pdf

'datr' cookies associated with their account proves the 'datr' cookie does more than identify a browser, but is also used by Facebook to personally-identify users.

c. The 'lu' cookie is used by Facebook to individually identify the last Facebook user to log-in to Facebook using the browser at issue.

d. The 'fr' cookie has a persistent value that is a combination of the encrypted browser identification and an encrypted version of a user's Facebook identification.[12]

83. Websites that design their pages in a way that permits Facebook to access these tracking cookies also send Facebook information on communications that users are making contemporaneous to users' communications with the websites. The websites do so through the process of re-direction explained above.

84. Facebook does not publicly disclose to web-developers that placing its "Like" or "Share" buttons on a web-page will automatically result in the website sending personally-identifiable information of the websites' users to Facebook connected to information about the communications between the users and the website.[13] *See* Exhibit D for a copy of Facebook's Developer pages.

85. Facebook uses the c_user, datr, lu, and fr cookies combined with the 'GET' requests, 'Referer headers', and other information, including, but not limited to, IP addresses, geographic identifiers, and personal information submitted by its users, to build detailed digital dossiers of each user.

86. Facebook acknowledges that it "scrapes" the pages of every website with social buttons "every 30 days to ensure the properties are up to date." Through this scraping process, Facebook knows the contents of communications made between users and websites not just

[12] See "Facebook Tracking Through Social Plug-ins," Technical Report prepared for the Belgian Privacy Commission, June 24, 2015. Available at: https://securehomes.esat.kuleuven.be/~gacar/fb_tracking/fb_plugins.pdf

[13] Facebook's public representations to web-developers regarding "plug-ins" like the "Like" and "Share" buttons can be found here: https://developers.facebook.com/docs/plugins

through GET requests and URLs, but also the entirety of communications sent from the websites back to each user.

87. Through the scraping process, Facebook has actual or constructive knowledge of the Privacy Policies at every website from which it tracks and intercepts user communications.

F. Facebook Ad Targeting by Medical Condition

88. As a result of its having collected the information set out above, Facebook then allows advertisers to directly-target ads to narrow segments of users identified with interests and actions in specified areas.

89. Facebook uses the data it obtains directly from users through tracking and monitoring their use of Facebook to sell advertising based on those communications and actions. Facebook's application for advertisers touts its ability to target users based on information Facebook has collected about them relating to health care.[14] For example, Facebook says it has identified more than 84 million users "who have expressed an interest in or like pages related to cancer awareness." It boasts more than 92 million people "who have expressed an interest in or like pages related to health care." Facebook also publicly claims to be able to allow advertisers to target ads to users "who have an interest in making donations to cancer causes" and to those who have an interest in "making donations to health causes."

90. Facebook boasts the ability to target advertising based on "Interests," telling advertisers, "Facebook can help you reach specific audiences by looking at their interests, activities, the Pages they have liked and closely related topics." A partial chart of medical category interest lists for sale for directing marketing of Facebook users in the United States is attached as Exhibit E, which contains a summary chart of the Facebook users in the United States which Facebook has placed in 154 separate medical categories for purposes of direct marketing.[15] The total number of individual U.S. Facebook users in these lists exceeds 255 million. Facebook's

[14] Facebook's application for advertisers can be found here: https://www.facebook.com/advertising

[15] Plaintiffs do not present Exhibit E as the entire universe of medical categories Facebook has created for direct marketing, but instead merely as the categories for which Plaintiffs' counsel searched.

medical conditions lists run the entire gamut of health conditions. There are 33 million Americans for the "cough and cold relief" list and 10,000 in the "ectopic pregnancy" list. Other lists include, but are not limited to: allergy relief, pregnancy, addiction, fever, cancer awareness, substance abuse awareness, diabetes management, back pain, vaginitis, lupus, gestational diabetes, Hepatitis C, bladder cancer, ADHD management, halitosis, rectal prolapse, cancer screening, HPV, diagnosis of HIV/AIDS, head and neck cancer, erectile dysfunction, and herpes simplex virus.

91. Plaintiffs are not aware of the total revenue Facebook derives from these lists, but, upon information and belief, avers that per user revenue for each medical list significantly exceeds the average per user revenue for non-medical lists.

G. Why Internet Tracking Is Not Anonymous for Facebook Even if Cookies Were Not Present

92. Facebook can track its users even without the presence of cookies.

93. Though industry insiders claim publicly that tracking is anonymous, experts disagree. For instance, in a widely cited blog post for The Center for Internet and Society at Stanford Law School titled "There is No Such Thing as Anonymous Online Tracking," Professor Arvind Narayanan explained:

> In the language of computer science, clickstreams – browsing histories that companies collect – are not anonymous at all; rather, they are pseudonymous. The latter term is not only more technically appropriate, it is much more reflective of the fact that at any point after the data has been collected, the tracking company might try to attach an identity to the pseudonym (unique ID) that your data is labeled with. Thus, identification of a user affects not only future tracking, but also retroactively affects the data that's already been collected. Identification needs to happen only once, ever, per user.
>
> Will tracking companies actually take steps to identify or deanonymize users? It's hard to tell, but there are hints that this is already happening: for example, many companies claim to be able to link online and offline activity, which is impossible without identity.[16]

94. Any company employing re-identification algorithms can precisely identify a particular consumer:

[16] "There is No Such Thing as Anonymous Online Tracking," Arvind Narayanan, July 28, 2011, published on the website of Stanford University Center for Internet and Society. Available at: http://cyberlaw.stanford.edu/blog/2011/07/there-no-such-thing-anonymous-online-tracking

> It turns out there is a wide spectrum of human characteristics that enable re-identification: consumption preferences, commercial transactions, Web browsing, search histories, and so forth. Their two key properties are that (1) they are reasonably stable across time and contexts, and (2) the corresponding data attributes are sufficiently numerous and fine-grained that no two people are similar, except with a small probability.
>
> The versatility and power of re-identification algorithms imply that terms such as "personally identifiable" and "quasi-identifier" simply have no technical meaning. While some attributes may be uniquely identifying on their own, any attribute can be identifying in combination with others.

95. The Federal Trade Commission has recognized the impossibility of keeping data derived from cookies and other tracking technologies anonymous, stating that industry, scholars, and privacy advocates have acknowledged that the traditional distinction between the two categories of data (personally identifiable information and anonymous information) has eroded and is losing its relevance.

96. Another technological innovation used to identify Internet users is called "browser fingerprinting," a process by which companies like Facebook "gather and combine information about a consumer's web browser configuration – including the type of operating system used and installed browser plug-ins and fonts – to uniquely identify and track the consumer."[17]

97. By using browser-fingerprinting alone, the likelihood that two separate users have the same browser-fingerprint is one in 286,777, or 0.000003487 percent.[18] This accuracy is increased substantially where the tracking company also records a user's IP address and unique device identifier.

98. Another recent innovation, as Prof. Narayanan predicted, is for companies to connect online dossiers with offline activity. As described by one industry insider:

> With every click of the mouse, every touch of the screen, and every add-to-cart, we are like Hansel and Gretel, leaving crumbs of information everywhere. With or without willingly knowing, we drop our places of residence, our relationship status, our circle of friends and even financial information. Ever wonder how sites like Amazon can suggest a new book you might like, or iTunes can match you up with an artist and even how

---

[17] *Protecting Consumer Privacy in an Era of Rapid Change* at 36.

[18] *How Unique Is Your Web Browser?* by Peter Eckersley, available at https://panopticlick.eff.org/browser-uniqueness.pdf. Visited July 28, 2014.

> Facebook can suggest a friend?
>
> Most tools use first-party cookies to identify users to the site on their initial and future visits based upon the settings for that particular solution. The information generated by the cookie is transmitted across the web and used to segment visitors' use of the website and to compile statistical reports on website activity. This leaves analytic vendors – companies like Adobe, Google, and IBM – *the ability to combine online with offline data*, creating detailed profiles and serving targeted ads based on users' behavior.[19]

99. Facebook can track its users even without accessing cookies on user computers. Every Facebook user provides Facebook with personally-identifiable information, including their first and last name and hometowns. Through their use of Facebook, they also provide Facebook with their contacts, email addresses, and likes.

100. Beyond user's names, email addresses, contacts, and likes, Facebook admits to collecting information about users' individual devices that it connects and intermingles with other account information, such as a user's name and email address:

> **Device information.**
> We collect information from or about the computers, phones, or other devices where you install or access our Services, depending on the permissions you've granted. We may associate the information we collect from your different devices, which helps us provide consistent Services across your devices. Here are some examples of the device information we collect:
>
> - Attributes such as the operating system, hardware version, device settings, file and software names and types, battery and signal strength, and device identifiers.
> - Device locations, including specific geographic locations, such as through GPS, Bluetooth, or WiFi signals.
> - Connection information such as the name of your mobile operator or ISP, browser type, language and time zone, mobile phone number and IP address.

101. Facebook connects this device and other information with the personal information users provide during sign-up and through use of Facebook.com.

---

[19] Tiffany Zimmerman, *Data Crumbs*, June 19, 2012, http://www.stratigent.com/community/analytics-insights-blog/data-crumbs (last visited September 16, 2013) (emphasis added).

102. Defendant Facebook's data industry rival Google has admitted that, armed with this information, even a simple IP address is personally-identifiable. On Google's Public Policy blog in 2008, then Google software engineer Alma Whitten explained:

> [I]s an IP address personal data, or, in other words, can you figure out who someone is from an IP address? A black-and-white declaration that all IP addresses are always personal data incorrectly suggests that every IP address can be associated with a specific individual. In some contexts this is more true: if you're an ISP and you assign an IP address to a computer that connects under a particular subscriber's account, and you know the name and address of the person who holds that account, then that IP address is more like personal data, even though multiple people could still be using it. On the other hand, the IP addresses recorded by every website on the planet without additional information should not be considered personal data, because these websites usually cannot identify the human beings behind these number strings.[20]

103. Facebook has more information about its members than the ISPs identified by Whitten have about their customers. Accordingly, to Facebook, IP addresses and unique device identifiers are personally-identifiable information.

H. Plaintiffs Are Without Knowledge Whether the Medical Defendants Were Aware of Facebook's Tracking and Interceptions

104. Defendants ACS, ASCO, MRF, Adventist, BJC, Cleveland Clinic and MD Anderson are aware of Facebook's ubiquitous presence on the Internet.

105. Plaintiffs are without knowledge as to whether Defendants ACS, ASCO, MRF, Adventist, BJC, Cleveland Clinic and MD Anderson are aware that Facebook tracks and intercepts communications between the Defendants and Internet users, including, in the case of the medical providers Adventist, BJC, Cleveland Clinic, and MD Anderson, their patients.

106. Plaintiffs are without knowledge as to whether Defendants ACS, ASCO, MRF, Adventist, BJC, Cleveland Clinic and MD Anderson profit directly or indirectly as a result of Facebook's tracking and interception of their communications to and from Internet users, including, in the case of the medical providers Adventist, BJC, Cleveland Clinic, and MD Anderson, their patients.

---

[20] See http://googlepublicpolicy.blogspot.com/2008/02/are-ip-addresses-personal.html. Viewed July 24, 2014.

I. Broken Privacy Promises at the Defendants' Medical Websites

1. Broken Privacy Promises at Cancer.org[21]

107. Users of Cancer.org trust that the American Cancer Society will not share the personal details of their cancer-related Internet search and browsing communications and activity on the American Cancer Society's website with third-parties.

108. Defendant ACS does not disclose any relationship with Facebook on its website.

109. Defendant ACS's Privacy Policy at Cancer.org begins by assuring users, "The American Cancer Society respects the privacy of every individual who uses ACS-owned websites[.]" *See* Exhibit F for a copy of ACS's Privacy Policy.

110. Defendant ACS next informs users that it collects two types of information. "Standard Web server traffic pattern information" which includes "[g]eneral traffic, site usage, browser information, and length of stay information" that "is collected and stored in log files" and which ACS promises "is *shared externally only on an aggregated basis*." And "[p]ersonal information" which ACS claims not to collect unless provided "voluntarily and knowingly."

111. ACS promises users it will only share health-related information and communications with third-parties in the following limited circumstances:

/ / /

/ / /

/ / /

/ / /

/ / /

/ / /

/ / /

/ / /

/ / /

/ / /

[21] http://www.cancer.org/aboutus/acspolicies/privacypolicies/internetprivacypolicies/internet-privacy-policy

External Use

Your health-related information is privileged and confidential and will not be shared or released to any organization or business entity other than those affiliated with or working in conjunction with ACS as follows:

1. We use third parties to provide you with the following services:
   1. Cancer Profiler: Disclosure of personal information is optional when using the cancer profiler. Additional services offered by NexCura are covered by their privacy policy and may require payment and disclosure.

   2. Clinical Trials: If you are considering clinical trial participation and would like to use the American Cancer Society Clinical Trials Matching Service, you must register with www.cancer.org and complete a screening questionnaire. This service is offered through a partnership between the American Cancer Society and the Coalition of Cancer Cooperative Groups. As part of the matching process, the Society and the Coalition will share your information with each other. If requested, the Society will then contact you to discuss the details or provide further information.

2. We occasionally make our constituent names and postal addresses available to other reputable non-profit organizations. We have found this to be the most cost-effective method of increasing our database of potential constituents and hope that you value the information they send you. Your name is only available to these carefully screened organizations for a limited time and it is de-identified, such that it is not associated with the American Cancer Society. Other organizations will not have continued access to your name and address unless you choose to respond to their initial mailing. We do not share email addresses or health related data. Information gathered as part of Cancer Profiler or Clinical Trials (above) is not shared.

3. We occasionally hire other companies to provide limited services on our behalf. We will only provide those companies the information they need to deliver the service and prohibit them from using that information for any other purpose.

4. We have relationships with companies that conduct charitable sales promotions and commercial coventures that support us in our mission and activities. If you provide us with your mailing address, we may pass your contact information to these companies so that they may ask you if you are interested in receiving their services. Your choice to use their services will benefit us; the amount of money we receive from these entities as a result of your participation is disclosed at the time you are contacted about the service. You are under no obligation to respond and the companies are restricted from using your contact information for any other purpose. Information gathered as part of Cancer Profiler or Clinical Trials (above) is not shared.

112. ACS does not disclose in any fashion that it shares its users' health-related communications and information with Defendant Facebook.

113. Facebook has actual and constructive knowledge of the Privacy Policy at Cancer.org that promises not to divulge to Facebook or any other third-party the details of users' "health-related information," including communications.

114. The policy is present on a publicly accessible page at Cancer.org which is scanned or available to be scanned by Facebook's web-crawlers and from which Facebook tracks, intercepts, and acquires communications.

115. Cancer.org does not contain Facebook "Like" buttons.

116. Despite the above-stated privacy promises, users of the Cancer.org website have their cancer-related search and browsing communications to and from the website disclosed to and tracked, intercepted, and acquired by Facebook connected to personally-identifiable information for each Plaintiff.

117. Plaintiff Winston Smith sought information, sent to, and received from Cancer.org communications relating to melanoma and cancer treatment using his mobile device:

http://m.cancer.org/treatment/supportprogramsservices/index

http://m.cancer.org/treatment/findingandpayingfortreatment/understandinghealthinsurance/healthinsuranceandfinancialassistanceforthecancerpatient/health-insurance-and-financial-assistance-toc

http://m.cancer.org/treatment/findingandpayingfortreatment/understandinghealthinsurance/prescriptiondrugassistanceprograms/prescription-drug-assistance-programs-toc

http://m.cancer.org/cancer/lungcancer-smallcell/detailedguide/small-cell-lung-cancer-after-lifestyle-changes

118. This communication contains information relating to the substance, purport, and meaning of the Plaintiff's communication. To state the obvious, Plaintiff Winston Smith sent and received communications with Cancer.org relating to lung cancer. In response, ACS sent back communications providing Plaintiff with the information sought.

119. Despite Cancer.org's Privacy Policy, the Plaintiff's communications to and from Cancer.org were contemporaneously re-directed to, tracked, intercepted, and acquired by Facebook through the process described above.

120. Upon these and other communications, Plaintiff's cancer-related communications were disclosed to, tracked, and intercepted by Facebook through cookies and other identifiers, including: c_user, lu, datr, fr, IP address, unique device identifiers, geographic locations, and browser-fingerprinting.

121. The exact content of Plaintiff's communications were disclosed to, tracked,

intercepted, and acquired by Facebook with a referer header containing the exact contents of Plaintiff's communications, including the exact contents of search queries Plaintiff made on the Cancer.org website.

2. Broken Privacy Promises at Cancer.net[22]

122. Users of Cancer.net trust that the American Society of Clinical Oncology will not share the personal details of their cancer-related Internet search and browsing communications and activity with ASCO with third-parties.

123. Defendant ASCO does not disclose any relationship with Facebook on its website.

124. The American Society of Clinical Oncology begins by assuring users it can be trusted with their personal information, stating, "We recognize that cancer is a personal disease, and we want you to feel as comfortable as possible visiting ASCO's websites[.]" *See* Exhibit G for a copy of ASCO's Privacy Policy.

125. In "Who Collects Information Through the Website," ASCO informs users:

> ASCO has engaged third party vendors to help us manage our web presence and allow us to better serve our web visitors. Personal information submitted to ASCO through third party managed pages may be shared with these vendors *as necessary for completing authorized transactions*. These third-party managed pages include the Journal of Clinical Oncology website (jco.ascopubs.org), the Journal of Oncology Practice website (jop.ascopubs.org), the Oncology Career Center website (www.careers.jco.org), portions of the Career Opportunities at ASCO page (www.asco.org/about-asco/working-asco), and portions of ASCO in Action (ascoaction.asco.org).

126. For users who visit Cancer.net "without registering," ASCO promises it "will only collect Non-Personal Information … about you through the use of first and third-party Cookies and other technical means."

127. ASCO informs users that "providers of third-party Cookies may have the ability to link your activities on the Website with your browsing activities elsewhere on the Internet." It then promises not to share PII with third-parties except under the following circumstances:

/ / /

[22] http://www.cancer.net/privacy-policy

5. Disclosure of Your Personally Identifiable Information

ASCO will only disclose your PII to third parties under the following circumstances:

- disclosure to corporate affiliates of ASCO, including the Conquer Cancer Foundation (www.conquercancerfoundation.org) and the Institute for Clinical Excellence, LLC;
- disclosure at your request, such as to complete transactions you undertake on the Website;
- disclosure to vendors engaged by ASCO to outsource one or more of our internal functions, products, or services, including but not limited to managing mailing lists, packaging, mailing and delivering purchases and promotional offers, consulting services, data modeling, printing, sending postal mail, and processing event registrations;
- disclosure of contact information to other ASCO members via our membership directories (the information made available in directories will not include will not include financial information, such as credit card or bank information, or social security numbers);
- disclosure of contact information to the public if you elect to participate in the Find an Oncologist Database (www.cancer.net/find-cancer-doctor);
- limited disclosure of contact information to trusted third parties to offer products and services to our members; and
- disclosure to private entities and law enforcement or other government officials as we, in our sole discretion, believe necessary or appropriate (a) to investigate or resolve possible problems or inquiries, (b) to conform to legal requirements or comply with legal process served on ASCO, (c) to protect our own business and assets, or (d) in special cases, such as a physical threat to you or others.

Please note that additional disclosure rules apply to information obtained by ASCO through the Oncology Career Center™, which is discussed further in Section 10.

Whenever ASCO discloses your PII to third parties, we will make commercially reasonable efforts to limit the information to which third parties have access and the purposes for which they can use it, as well as to require that the recipients thereof apply the terms of this Privacy Policy to that information as if they were ASCO.

128. Cancer.net does not disclose in any fashion that it shares users' health-related information with Defendant Facebook.

129. Facebook has actual and constructive knowledge of the Privacy Policy at Cancer.net that promises not to divulge details of user communications with ASCO to Facebook.

130. The policy is present on a publicly-accessible page at Cancer.net which is scanned or available to be scanned by Facebook's web-crawler and from which Facebook tracks, intercepts, and acquires communications.

131. Cancer.net does not contain Facebook "Like" buttons.

132. Plaintiff Winston Smith sought information, sent to, and received from Cancer.net communications relating to melanoma and cancer treatment:

http://www.cancer.net/navigating-cancer-care/financial-considerations/financial-resources
http://www.cancer.net/cancer-types/melanoma/treatment-options
http://www.cancer.net/navigating-cancer-care/diagnosing-cancer/tests-and-procedures/positron-

emission-tomography-pet-scan

133. These communications contain information relating to the substance, purport, and meaning of the Plaintiff's communications. To state the obvious, Plaintiff Winston Smith sent and received communications from Cancer.net relating to (1) financial considerations for cancer, (2) treatment options for melanoma, and (3) the positron emission tomography pet scan test for detecting cancer.

134. Despite Cancer.net's privacy promises, the Plaintiff's communications to and from Cancer.net were contemporaneously re-directed, tracked, intercepted, and acquired by Facebook through the process described above.

135. Upon these and other communications, Plaintiff's cancer-related communications were disclosed to, tracked, intercepted, and acquired by Facebook through cookies and other identifiers including: c_user, lu, datr, fr, IP address, unique device identifiers, geographic locations, and browser-fingerprinting.

136. The exact content of Plaintiff's communications were disclosed to, tracked, intercepted, and acquired by Facebook with a referer header containing the exact contents of Plaintiff's communications, including the exact contents of search queries Plaintiff made on the Cancer.net website.

3. Broken Privacy Promises at Melanoma.org[23]

137. Users of Melanoma.org trust that Defendant Melanoma Research Foundation will not share the personal details of their cancer-related Internet search and browsing communications and activity on the MRF website with third-parties.

138. Defendant MRF does not disclose any relationship with Facebook on its website.

139. Defendant MRF's Privacy Policy at Melanoma.org begins by assuring users, "The Melanoma Research Foundation is committed to protecting your privacy." *See* Exhibit H for a copy of MRF's Privacy Policy.

140. MRF defines "personal data" to mean "data that allows someone to identify or

[23] http://www.melanoma.org/privacy-policy

contact you, including, for example, your name, address, telephone number, e-mail address, as well as any other non-public information about you that is associated with or linked to any of the foregoing data."

141. MRF discloses that it uses cookies to track users for itself.

142. MRF promises the following regarding disclosures to third-parties:

> **6.2 Disclosure to Third Party Service Providers and Third Party Companies.** Except as otherwise stated in this policy, we do not generally sell, trade, share, or rent the Personal Data collected from our services to other entities. However, we may share your Personal Data with third party service providers to provide you with the Service; to conduct quality assurance testing; to facilitate creation of accounts; to provide technical support; to send you our online newsletter, to enable online donations, or to provide other services. These third party service providers are required not to use your Personal Data other than to provide the services requested by the MRF. You expressly consent to the sharing of your Personal Data with our contractors and other service providers for the sole purpose of providing services to you. We do not sell or share your Personal Data with Third Party Companies.

143. MRF does not disclose in any fashion that it shares its users' health-related communications and information with Facebook.

144. Facebook had actual and constructive knowledge of the Privacy Policy at Melanoma.org that promises not to divulge to Facebook their users' personal data.

145. The policy is present on a publicly accessible page at Melanoma.org which is scanned or available to be scanned by Facebook's web-crawlers and from which Facebook tracks, intercepts, and acquires communications.

146. Despite the above-stated privacy promises, users of the Melanoma.org website have their cancer-related search and browsing communications to and from the website disclosed to, tracked, intercepted, and acquired by Facebook connected to information that is personally-identifiable for each plaintiff.

147. Plaintiff Winston Smith sought information, sent to, and received from Melanoma.org communications relating to the diagnosis of melanoma:

http://www.melanoma.org/find-support/patient-community/mpip-melanoma-patients-information-page/baking-soda

148. This communication contains information relating to the substance, purport, and

meaning of the Plaintiff's communications. To state the obvious, Plaintiff Winston Smith sent and received communications with Melanoma.org relating to Melanoma and treatment with baking soda. In response, MRF sent back communications providing the Plaintiffs' with the information sought.

149. Despite Melanoma.org's Privacy Policy, the Plaintiff's communications to and from Melanoma.org were contemporaneously re-directed to, tracked, intercepted, and acquired by Facebook through the process described above.

150. Upon these and other communications, Plaintiff's cancer-related communications were disclosed to, tracked, and intercepted by Facebook through cookies and other identifiers, including: c_user, lu, datr, fr, IP address, unique device identifiers, geographic locations, and browser-fingerprinting. These same communications were also acquired by Adobe through the use of cookies and other identifiers.

151. The exact content of Plaintiff's communications were disclosed to, tracked, intercepted, and acquired by Facebook with a referer header containing the exact contents of Plaintiff's communications, including the exact contents of search queries Plaintiff made on the Melanoma.org website.

4. Broken Privacy Promises at ShawneeMission.org and Other Adventist Websites

152. ShawneeMission.org is the website for Defendant Adventist Health System's hospital in Shawnee Mission, Kansas known as Shawnee Mission Hospital.

153. Users of ShawneeMission.org, including patients of Shawnee Mission Hospital, trust that Shawnee Mission and their health care providers will not disclose the personal details of their health-related Internet communications to third-parties.

154. Defendant Adventist creates a record of all health-related communications it receives from and sends to Internet users, many of whom include its own patients, and connect the communications to individual users through IP addresses and first-party cookies, including but not limited to:

a. atrfs;

b. atuvc;

c. atuvs;

d. utma;

e. utmb;

f. utmc; and

g. utmz.

155. Defendant Adventist does not disclose in any fashion that it shares users' health-related communications with Shawnee Mission with Facebook.

156. Defendant Adventist promises not to share personally-identifiable information of its patients and website users with third-parties except in limited circumstances which do not apply. See Exhibit I for a copy of the ShawneeMission.org Privacy Policy which states:

> As a general rule, we will not disclose your personally identifiable information to any unaffiliated third party, except when we have your permission or under special circumstances, such as when we need to treat the information collected through this website as an asset in the event of the merger of sale of Adventist, or a portion of our business. Your personally identifiable information may be accessed by our management information services team or an affiliated third party providing technical support or maintenance for us.
>
> If we offer services using or in conjunction with an unaffiliated third party, we may need to share some or all of your personally identifiable information with that unaffiliated third party for purposes of providing the services to you. If you do not want your personally identifiable information to be shared, you can choose not to use that particular service or notify us that you do not wish your personally identifiable information to be shared. In some circumstances we may be required by law to disclose personally identifiable information. We will do so, in good faith, only to the extent we believe to be required by law. We may also disclose personally identifiable information in special cases when we have reason to believe that disclosing this information is necessary to identify, contact or bring legal action against a third party who may be violating our terms and conditions governing the use of our website, or who may be (intentionally or unintentionally) causing injury to or interference with your or our rights or property or those of a third party.
>
> We may share anonymous information with third parties. For example, we may match our user information, such as gender and age preferences and usage, with data of these third parties to help develop additional products and services to offer through our website.

157. Defendant Adventists' other hospital websites, including but not limited to, keepingyouwell.com, ctmc.org, chippewavalleyhospital.com, gordonhospital.com, manchestermemorial.com, mplex.org, porterhospital.org, takoma.org, texashealthhugeley.org, texashealth.org ("other Adventist hospital websites"), maintain substantially similar privacy policies.

158. Facebook has actual and constructive knowledge of the Privacy Policy at ShawneeMission.org and the other Adventist hospital websites that fail to disclose the divulgence to Facebook of the details of users' and patients' Internet communications.

159. The ShawneeMission.org Privacy Policy, and other Adventist hospital website privacy policies, are present on publicly-accessible pages which are scanned or available to be scanned by Facebook's web-crawler and from which Facebook tracks and intercepts communications.

160. Despite the above-stated privacy promises, users of the ShawneeMission.org website and the other Adventist hospital websites have their health-related search and browsing communications to and from Defendant Adventist disclosed to, tracked, intercepted, and acquired by Facebook connected to information which personally-identifies each plaintiff.

161. Plaintiff Jane Doe sought information, sent to, and received from ShawneeMission.org communications relating to pain management and her particular doctor:

http://www.shawneemission.org/health-services/center-for-pain-medicine#.VLk-FHv_4uM

http://www.shawneemission.org/orthopedic-spine-center#.VLk-R3v_4uN

http://www.shawneemission.org/find-a-doctor?doctor=Scott-E-Ashcraft-MD-1407822869#.U77dgKhRa-k

162. These communications contain information relating to the substance, purport, and meaning of Jane Doe's communications. To state the obvious, Plaintiff Jane Doe was sending and receiving communications to and from Adventist relating to pain and medical treatment by Dr. Scott Ashcraft at Shawnee Mission. In response to these communications requesting information, Defendant Adventist sent back essay communications providing Jane Doe with the information sought.

163. Despite Adventist's privacy promises, the Plaintiff's communications to and from ShawneeMission.org and the other Adventist hospital websites were contemporaneously re-directed, tracked, intercepted, and acquired by Facebook through the process described above.

164. Upon these and other communications, Plaintiff's health-related communications were disclosed to, tracked, intercepted, and acquired by Facebook through cookies and other identifiers, including: c_user, lu, datr, fr, IP address, unique device identifiers, geographic locations, and browser-fingerprinting.

165. The exact content of Plaintiff's communications were disclosed to, tracked, intercepted, and acquired by Facebook with a referer header containing the exact contents of the Plaintiff's communications, including the exact contents of search queries Plaintiff made on the Adventist websites.

5. Broken Privacy Promises at BarnesJewish.org

166. BarnesJewish.org is the website for Defendant BJC Healthcare. Users of BarnesJewish.org trust that BJC Healthcare will not disclose the personal details of their health-related Internet communications with BJC to third-parties.

167. Defendant BJC creates a record of all health-related communications it receives from and sends to Internet users and connects the communications to individual users through IP addresses, unique device identifiers, and first-party cookies, including:

a. _utma;

b. _utmb;

c. _utmc;

d. _utmz;

e. _ga; and

f. _ibp_phone_number.

168. Defendant BJC does not disclose in any fashion that it shares users' and patients' health-related communications with Facebook.

169. Defendant BJC's Privacy Policy at BarnesJewish.org assures users that it complies

with the Health Insurance Portability and Accountability Act of 1996 (HIPAA).[24] It then promises, "We are required by law to protect the privacy of your protected health information." It defines "protected health information" to include "information that [BJC] create[s] or receive[s] that identifies you and your past, present or future health status or care[.]"

170. BJC notifies users that it discloses health information without written consent or authorization for the purposes of treatment, payment of health services, health care operations, or other special circumstances which are not present in this case.

171. A separate document[25] provides further details on BJC privacy on the Internet. *See* Exhibit J for a copy of BJC's Privacy Policy. It explains:

> PRIVACY STATEMENT
>
> Barnes-Jewish Hospital has created this statement to demonstrate our commitment to your privacy. This statement explains our information-gathering and dissemination practices for this Web site.
>
> A typical visit to our Web site does not require a user to submit personal information. However, if you decide to send us an e-mail, respond to a survey, or subscribe to an online publication with your contact information, we will respond to you with the information you request and other information that we think might be of interest to you. If you choose to receive more information, your name and contact information (including e-mail address) will be added to our database. From that database, we may send you materials such as newsletters, brochures or articles of interest via regular mail, e-mail or in other ways.
>
> Information you submit may be routinely shared with our parent organization, BJC HealthCare as they often distribute our materials, or with the Washington University School of Medicine if you are looking for a physician referral. Other than these two organizations, we will only forward your personal information to organizations working on our behalf. We urge you not to provide any confidential information about you or your health to us via electronic communication. If you do so, it is at your own risk. Although we attempt to maintain or computer network in a secure manner to protect the content of your messages, we cannot provide absolute assurance that the contents of your e-mail will not become accessible to individuals or entities that are not authorized to access your information.
>
> The first visit you make to the Barnes-Jewish Hospital Web site places a "cookie" on your computer. A cookie is a file used to personalize the Web site for you based on your initial and subsequent visits. The cookie will allow you to see or not to see items upon subsequent visits. This technology is not intended to identify you to us in any way; however, it can be used to serve ads to you based on your visit to our site. Click here to learn more about opting out of data collection by Google Analytics, or, click here to customize Google display network ad settings for your browser.

[24] See http://www.barnesjewish.org/legal/hipaa-notice. Last visited April 10, 2015.

[25] See http://www.barnesjewish.org/?id=96&sid=1. Last visited April 10, 2015.

172. Facebook has actual and constructive knowledge of the Privacy Policy at BarnesJewish.org that promises not to divulge details of user communications to Facebook.

173. The policy is present on publicly accessible pages at BarnesJewish.org which is scanned or available to be scanned by Facebook's web-crawler and from which Facebook tracks and intercepts communications.

174. Despite the above-stated privacy promises, users of the BarnesJewish.org website have their health-related search and browsing communications to and from BJC disclosed to, tracked, and intercepted by Facebook connected to information that personally-identifiable for each plaintiff.

175. Plaintiff Jane Doe II sought information, sent to, and received from BarnesJewish.org communications relating to a sensitive medical condition, and her husband's doctor:

http://www.barnesjewish.org/physicians/details.aspx?physician=1033041

http://www.barnesjewish.org/physicians/details.aspx?physician=1027051

176. These communications contain information relating to the substance, purport, and meaning of the Plaintiff's communications. To state the obvious, Plaintiff Jane Doe II was sending and receiving communications to and from BarnesJewish.org relating to her family's health care treatment and their doctors: Steven R. Hunt, M.D. (identified on the BJC website as "1033041") and Sudhir Jain, M.D. ("1027051"). In response to these communications requesting information, Defendant BJC sent back communications providing the Plaintiff with the information sought.

177. Plaintiff Jane Doe II's husband was a patient at BJC.

178. Despite BJC's privacy promises, the Plaintiff's communications to and from BarnesJewish.org were contemporaneously re-directed, tracked, intercepted, and acquired by Facebook through the process described above.

179. Upon these and other communications, Plaintiff's health-related communications were disclosed to, tracked, intercepted, and acquired by Facebook through the following cookies and other identifiers: c_user, lu, datr, fr, IP address, unique device identifiers, geographic locations, and browser-fingerprinting. These same communications were also acquired by Twitter

through the use of cookies and other identifiers.

180. The exact content of Plaintiff's communications were disclosed to, tracked, intercepted, and acquired by Facebook with a referer header containing information relating to the substance, purport, or meaning of Plaintiff's communications, including the exact contents of search queries Plaintiff made on the BarnesJewish.org website.

6. Broken Privacy Promises at ClevelandClinic.org

181. ClevelandClinic.org is the website for Defendant Cleveland Clinic. Users of ClevelandClinic.org trust that the Cleveland Clinic will not disclose the personal details of their health-related Internet communications with Cleveland Clinic to third-parties.

182. Defendant Cleveland Clinic creates a record of all health-related communications it receives from and sends to Internet users, many of whom include its own patients, and connects the communications to individual users through IP addresses, unique device identifiers, and first-party cookies, including:

a. _utma;

b. _utmz;

c. _mkto_trk;

d. ClrOSSID;

e. ClrSCD; and

f. CLrSSID.

183. Defendant Cleveland Clinic does not disclose in any fashion that it shares' users and patients' health-related communications with Facebook.

184. Defendant Cleveland Clinic makes an unequivocal promise about the privacy of its Internet users. *See* Exhibit K for a copy of Cleveland Clinic's Privacy Policy, which states:[26]

> **PERSONAL INFORMATION.**
>
> A visitor can access and browse our entire site at any time without providing any personal information. We do not collect information that would personally identify you unless you choose to provide it.
>
> In addition, Cleveland Clinic does not share any personally identifiable information of any individual with any third party unrelated to Cleveland Clinic, except in situations where we must provide information for legal purposes or investigations, or if so directed by the patient through a proper authorization.

[26] See http://my.clevelandclinic.org/about-cleveland-clinic/about-this-website/privacy-security

185. Facebook has actual and constructive knowledge of the Privacy Policy at ClevelandClinic.org that promises not to divulge to Facebook, or any other third-party unrelated to Cleveland Clinic, user communications with Cleveland Clinic.

186. The Cleveland Clinic Privacy Policy is present on a publicly-accessible page at ClevelandClinic.org which is scanned or available to be scanned by Facebook's web-crawler and from which Facebook tracks, intercepts, and acquires communications.

187. Despite the above-stated privacy promises, users of the ClevelandClinic.org website have their health-related search and browsing communications to and from Cleveland Clinic disclosed to, tracked, intercepted, and acquired by Facebook connected to information that personally-identifies each plaintiff.

188. Plaintiff Jane Doe II sought information, sent to, and received from ClevelandClinic.org communications relating to intestine transplants:

http://my.clevelandclinic.org/search/results?q=intestine%20transplant

189. This communication contains information relating to the substance, purport, and meaning of the Plaintiff's communication. To state the obvious, Plaintiff Jane Doe II was sending and receiving communications to and from ClevelandClinic.org relating to intestine transplants. In response to this communication, Defendant Cleveland Clinic sent back communications providing the Plaintiff with the information sought.

190. Despite Cleveland Clinic's privacy promises, the Plaintiff's communications to and from ClevelandClinic.org were contemporaneously re-directed, tracked, intercepted, and acquired by Facebook through the process described above.

191. Upon these and other communications, Plaintiff's health-related communications were disclosed to, tracked, intercepted, and acquired by Facebook through the following cookies and other identifiers, including: c_user, lu, datr, fr, IP address, unique device identifiers, geographic locations, and browser-fingerprinting.

192. The exact content of Plaintiff's communications were disclosed to, tracked, intercepted, and acquired by Facebook with a referer header containing the exact contents of the Plaintiff's communications, including the exact contents of search queries Plaintiff made on the

ClevelandClinic.org website.

7. Broken Privacy Promises at MDAnderson.org

193. MDAnderson.org is the website for Defendant University of Texas MD Anderson Cancer Center. Users of MDAnderson.org trust that it will not disclose the personal details of their health-related Internet communications with MD Anderson to third-parties.

194. Defendant MD Anderson creates a record of all health-related communications it receives from and sends to Internet users, many of whom include its own patients, and connect the communications to individual users through IP addresses, unique device identifiers, and first-party cookies including:

a. _utma;

b. _utmz;

c. s_nr;

d. s_vi; and

e. fsr.r.

195. Defendant MD Anderson does not disclose in any fashion that it shares users' and patients' health-related communications with Facebook.

196. Defendant MD Anderson's Privacy Policy assures users that it complies with HIPAA. It defines "protected health information" to include "any information, whether oral, written or recorded in electronic form, that is created or received by us as health care providers that identifies you and relates to your past, present or future physical or mental health or condition, treatment, or payment for your healthcare."[27]

197. MDAnderson makes an unequivocal promise about the privacy of its Internet users. *See* Exhibit L for copy of MDAnderson's Privacy Policy. It states, in bold-faced type on its website Privacy Policy[28] page:

[27] See http://www.mdanderson.org/about-us/legal-and-policy/legal-statements/legal-statements-joint-notice-of-privacy-practices.html. Last visited December 9, 2015.

[28] See http://www.mdanderson.org/about-us/legal-and-policy/site-policies/site-policies-privacy-policy.html. Last visited December 9, 2015.

> **Under no circumstances will we ever disclose (to a third party) personal information about individual medical conditions or interests, except when we believe in good faith that the law requires it.**

198. Facebook has actual and constructive knowledge of the Privacy Policy at MDAnderson.org that promises not to divulge details of user communications to Facebook.

199. MD Anderson's Privacy Policy is present on a publicly accessible page at MDAnderson.org which is scanned or available to be scanned by Facebook's web-crawlers and from which Facebook tracks, intercepts, and acquires communications.

200. MDAnderson does not contain Facebook "Like" buttons.

201. Despite the above-stated privacy promises, users of the MDAnderson.org website have their health-related search and browsing communications to and from MD Anderson disclosed to, tracked, intercepted, and acquired by Facebook connected to information that personally-identifies each plaintiff.

202. Plaintiff Winston Smith sought information, sent to, and received from MDAnderson.org communications relating to metastatic melanoma: http://www2.mdanderson.org/cancerwise/2012/06/metastatic-melanoma-a-wife-reflects-on-husbands-shocking-diagnosis.html

203. This communication contains information relating to the substance, purport, and meaning of the Plaintiff's communication. To state the obvious, Plaintiff Winston Smith was sending and receiving communications to and from MDAnderson.org relating to "metastatic melanoma." In response to this communication, Defendant MDAnderson sent back communications providing Plaintiff Winston Smith with the information sought.

204. Despite MDAnderson's privacy promises, the Plaintiff's communications to and from MDAnderson.org were contemporaneously re-directed, tracked, intercepted, and acquired by Facebook through the process described above.

205. Upon this and other communications, Plaintiff's health and cancer-related communications were disclosed to, tracked, intercepted, and acquired by Facebook through the following cookies and other identifiers: c_user, lu, datr, fr, IP address, unique device identifiers,

geographic locations, and browser-fingerprinting.

206. The exact content of Plaintiff's communications were disclosed to, tracked, intercepted, and acquired by Facebook with a referer header containing the exact contents of Plaintiff's communications, including the exact contents of search queries Plaintiff made on the MDAnderson.org website.

J. Application of HIPAA to the Actions of the Health Care Provider Defendants

207. The Health Insurance Portability and Accountability Act protects the privacy of medical records. It was enacted to establish "for the first time, a set of basic national privacy standards and fair information practices that provides all Americans with a basic level of protection and peace of mind that is essential to their full participation in their care." Accordingly, HIPAA "sets a floor of ground rules for health care providers … to follow, in order to protect patients and encourage them to seek needed care."[29]

208. Under HIPAA, "A covered entity or business associate may not use or disclose protected health information, except as permitted" by HIPAA. 45 C.F.R. §164.502. "Protected health information" is defined as "individually identifiable health information that is transmitted by electronic media, maintained in electronic media, or transmitted or maintained in any other form of media." 45 C.F.R. § 160.103. "Health information" is defined as "any information … whether oral or recorded in any form or medium that … (1) is created or received by a health care provider … and (2) [r]elates to the past, present, or future physical or mental health or condition of *an individual*[.]" 45 C.F.R. § 160.103. "Individual" under HIPAA is not limited to current or former patients of the covered entity, but is instead defined as "the person who is the subject of protected health information."

209. Whether information is "individually identifiable" under HIPAA is governed by 45 C.F.R. §164.514, which sets forth a list of "identifiers" that must be "removed" before a covered entity may determine that the information "is not individually identifiable health information." 45 C.F.R. § 164.514(b). The list of "identifiers" which must be removed includes the following

[29] See Standards for Privacy of Individually Identifiable Health Information, 65 Fed. Reg. 82,462-64 (Dec. 28. 2000).

"identifiers of the individual or of relatives … or household members of the individual:"

a. Names, § 164.514(b)(2)(i)(A);

b. All geographic subdivisions smaller than a state, § 164.514(b)(2)(i)(B);

c. Device identifiers and serial numbers, § 164.514(b)(2)(i)(M);

d. Web Universal Resource Locators (URLs), § 164.514(b)(2)(i)(N);

e. Internet Protocol (IP) address numbers, § 164.514(b)(2)(i)(O); and

f. Any other unique identifying number, characteristic, or code [with an inapplicable exception], §164.514(b)(2)(i)(R).

210. A "covered entity must obtain an authorization for any use or disclosure of protected health information for marketing" with two inapplicable exceptions. 45 C.F.R. § 164.508(3)(i). "Marketing" is defined as "to make a communication about a product or service that encourages recipients of the communication to purchase or use the product or service[.]" 45 C.F.R. § 164.501.

211. A "covered entity must obtain an authorization for any disclosure of protected health information which is a sale of protected health information[.]" 45 C.F.R. § 164.508(4)(i). The "sale of protected health information" means "a disclosure of protected health information by a covered entity … where the covered entity … directly or indirectly receives remuneration from or on behalf of the recipient of the protected health information in exchange for the protected health information[.]" 45 C.F.R. § 164.502(a)(5)(ii)(B).

212. A valid HIPAA authorization must contain:

a. A description of the information to be used or disclosed that identifies the information in a specific and meaningful fashion;

b. The name or other specific identification of the person(s), or class of persons, authorized to make the requested use or disclosure;

c. The name or other specific identification of the person(s), or class of persons, to whom the covered entity may make the requested use or disclosure;

d. A description of each purpose of the requested use or disclosure;

e. An expiration date or an expiration event that relates to the individual or the purpose of the use or disclosure;

f. The signature of the individual and the date;

g. Notice of the individual's right to revoke the authorization in writing; the covered entity's ability or inability to condition treatment, payment, enrollment, or eligibility for benefits on the authorization; and the potential for information disclosed to be subject to re-disclosure by the recipient;

h. The authorization must be written in plain language; and

i. The covered entity must provide the individual with a copy of the signed authorization.

213. HIPAA violations are subject to civil and criminal penalties. The civil penalty for an unknowing HIPAA violation is a fine between $100 and $50,000 for each violation with an aggregate cap of $1.5 million "for identical violations during a calendar year." 45 C.F.R. § 160.404(b)(2). The criminal provisions contained in 42 U.S.C. § 1320d-6 specify:

> **(a) Offense**
>
> A person who knowingly and in violation of this part—
>
> **(1)** uses or causes to be used a unique health identifier;
>
> **(2)** obtains individually identifiable health information relating to an individual; or
>
> **(3)** discloses individually identifiable health information to another person,
>
> shall be punished as provided in subsection (b) of this section. For purposes of the previous sentence, a person (including an employee or other individual) shall be considered to have obtained or disclosed individually identifiable health information in violation of this part if the information is maintained by a covered entity (as defined in the HIPAA privacy regulation described in section 1320d-9 (b)(3) of this title) and the individual obtained or disclosed such information without authorization.
>
> **(b) Penalties**
>
> A person described in subsection (a) of this section shall—
>
> **(1)** be fined not more than $50,000, imprisoned not more than 1 year, or both;
>
> **(2)** if the offense is committed under false pretenses, be fined not more than $100,000, imprisoned not more than 5 years, or both; and
>
> **(3)** if the offense is committed with intent to sell, transfer, or use individually identifiable health information for commercial advantage, personal gain, or malicious harm, be fined not more than $250,000, imprisoned not more than 10 years, or both.

214. Defendants Adventist, BJC, Cleveland Clinic and MD Anderson are "covered entities" governed by HIPAA.

215. The named-Plaintiffs and the classes are "individuals" protected by HIPAA with respect to their communications with covered entities.

216. The Plaintiffs' communications with the covered entities constitutes "protected health information."

a. The information accessed and Plaintiffs' communications sent to and received from ShawneeMission.org and the other Adventist hospital websites , BarnesJewish.org, ClevelandClinic.org, MDAnderson.org that were, respectively, created by Adventist, BJC, Cleveland Clinic, and MD Anderson. Further, the plaintiffs' communications with these websites were recorded by Adventist, BJC, Cleveland Clinic and MD Anderson in a form that was created and received by each respective Defendant. In particular, the covered entity websites each tracked, created, and recorded logs of the Plaintiffs' activities on the health care websites through the websites' own use of cookies and other personally-identifying information including, but not limited to, device identifiers and IP addresses.

b. The Plaintiffs' communications with Adventist, BJC, Cleveland Clinic, and MD Anderson related to their "past, present, and future physical or mental health or condition."

c. The information tracked, created, and recorded by Adventist, BJC, Cleveland Clinic, and MD Anderson included:

i. Geographic subdivisions smaller than a state;

ii. Device identifiers and/or serial numbers;

iii. Web Universe Resource Locators (URLs);

iv. IP addresses; and

v. Other unique identifying numbers, characteristics, or codes – including, but not limited to, Internet cookies.

217. Adventist, BJC, Cleveland Clinic and MD Anderson, whether purposefully or negligently, designed their websites in a manner that disclosed to Facebook the communications Plaintiffs sent to and received from them.

218. The disclosures included details on the communication through referer headers and GET requests with sensitive information relating to "past, present, or future" medical conditions.

219. Defendant Facebook learned further details of the communications through its web-crawlers.

220. The disclosures to Facebook also included personally-identifiable information attached to the sensitive medical information. This PII took the form of geographic subdivisions smaller than a state, device identifiers and/or serial numbers, URLs, IP addresses, and other unique identifying numbers, characteristics, and codes – including but not limited to Internet cookies.

221. Adventist, BJC, Cleveland Clinic, and MD Anderson failed to obtain the express written authorization required by HIPAA for disclosure relating to marketing, sale, or any other purpose not specifically exempted by HIPAA.

222. Facebook has actual or constructive knowledge that Defendants Adventist, BJC, Cleveland Clinic, and MD Anderson are health care providers and covered entities under HIPAA.

223. Defendants Adventist, BJC, Cleveland Clinic and MD Anderson reference HIPAA policies on their websites.

224. The websites of Adventist, BJC, Cleveland Clinic and MD Anderson, are scanned or available to be scanned by Facebook's web-crawler.

225. Because Adventist, BJC, Cleveland Clinic and MD Anderson did not receive the express written consent of the Plaintiffs, in addition to violating various other state and criminal laws, the actions and processes described in this complaint violated HIPAA.

K. California Civil Code Section 1798.91 – Consent for Direct Marketing Based on Medical Information

226. California Civil Code section 1798.91 provides that "[a] business may not request in writing medical information directly from an individual regardless of whether the information pertains to the individual or not, and use, share or otherwise disclose that information for direct

marketing purposes" unless it first "disclose[s] in a clear and conspicuous manner that it is obtaining the information to market or advertise products, goods, or services to the individual" and "obtain[s] the written consent of the individual to whom the information pertains … to permit his or her medical information to be used or shared to market or advertise products, goods, or services to the individual."

227. Facebook is a business.

228. Per Cal. Civ. Code § 1798.91(a)(1), "direct marketing purposes" means "the use of personal information for marketing or advertising products, goods, or services directly to individuals." Facebook collects information from Plaintiffs and their computing devices for purposes of direct marketing and advertising products, goods, and services at Facebook.com.

229. Per Cal. Civ. Code § 1798.91(a)(2), "medical information" means "any individually identifiable information, in electronic or physical form, regarding the individual's medical history, or medical treatment or diagnosis by a health care professional." "Individually identifiable" means "the medical information includes of contains any element of personal identifying information sufficient to allow identification of the individual, such as the individual's name, address, electronic mail address, telephone number, or social security number, or other information that, alone or in combination with other publicly available information, reveals the individual's identity." The definition of "medical information" includes an exception, and "does not mean a subscription to, purchase of, or request for a periodical, book, pamphlet, video, audio, or other multimedia product or non-profit association information."

230. The Plaintiffs' communications with the health care Defendants contain "medical information" which is individually identifiable and protected by Cal. Civ. Code § 1798.91(a)(2). This collection by Facebook includes communications seeking details on specific health care providers, i.e. doctors, employed by medical websites and entities covered by HIPAA. It also includes the mere fact that Plaintiffs are making communication with the health care Defendant and/or any of its specialties or that they are seeking information on how to make payments. For example, Facebook collects information from the Plaintiffs regarding their communication with BJC on the following webpages:

- http://www.barnesjewish.org/
- http://www.barnesjewish.org/physicians/
- http://www.barnesjewish.org/physicians/results.aspx?find=liver
- https://www.barnesjewish.org/requestappointment/
- http://www.barnesjewish.org/cancer-center
- http://www.barnesjewish.org/physicians/details.aspx?physician=1022180
- http://www.bjc.org/For-Patients-Visitors/Financial-Assistance-Billing-Resources/Online-Bill-Pay

Substantially similar communications are taken and recorded by Facebook at the other health care Defendants and other websites of "covered entities" under HIPAA. These communications relate to the Plaintiffs' "medical history, or medical treatment or diagnosis by a health care professional" protected by Cal. Civ. Code § 1798.91(a)(2).

231. Facebook collects the Plaintiffs' communications with the health care Defendants without Plaintiffs' knowledge or consent through the use of computer code designed by Facebook that instructs the health care Defendants webpages to re-direct the Plaintiffs' communications to Facebook from the Plaintiffs' web-browsers.

232. Plaintiffs' interests and activities on Facebook are also collected directly by Facebook and used to place the Plaintiffs into medical interest categories for purposes of direct marketing. These interests and activities relating to Plaintiffs' or another individual's "medical history or medical treatment or diagnosis by a health care professional" is "medical information" protected by Cal. Civ. Code § 1798.91(a)(2).

233. Per Cal. Civ. Code § 1798.91(a)(3), "clear and conspicuous" means "in larger type than the surrounding text, or in contrasting type, font, or color to the surrounding text of the same size, or set off from the surrounding text of the same size by symbols or other marks that call attention to the language." Facebook did not make any disclosures that it tracks and takes medical information of the Plaintiffs for purposes of direct marketing. To the extent it claims it provided any such disclosure, it did not do so in a "clear and conspicuous" manner. Facebook makes the following statements in its Data Policy about using the information it collects directly from its

users for purposes of direct marketing.

> **Show and measure ads and services.**
> We use the information we have to improve our advertising and measurement systems so we can show you relevant ads on and off our Services and measure the effectiveness and reach of ads and services. Learn more about advertising on our Services and how you can control how information about you is used to personalize the ads you see.

> **Advertising, Measurement and Analytics Services (Non-Personally Identifiable Information Only).**
> We want our advertising to be as relevant and interesting as the other information you find on our Services. With this in mind, we use all of the information we have about you to show you relevant ads. We do not share information that personally identifies you (personally identifiable information is information like name or email address that can by itself be used to contact you or identifies who you are) with advertising, measurement or analytics partners unless you give us permission. We may provide these partners with information about the reach and effectiveness of their advertising without providing information that personally identifies you, or if we have aggregated the information so that it does not personally identify you. For example, we may tell an advertiser how its ads performed, or how many people viewed their ads or installed an app after seeing an ad, or provide non-personally identifying demographic information (such as 25 year old female, in Madrid, who likes software engineering) to these partners to help them understand their audience or customers, but only after the advertiser has agreed to abide by our advertiser guidelines.
>
> Please review your advertising preferences to understand why you're seeing a particular ad on Facebook. You can adjust your ad preferences if you want to control and manage your ad experience on Facebook.

234. Facebook also does not obtain written consent to collect medical information for purposes of direct marketing. Facebook's Terms, Data Policy, and Cookie use pages do not

apprise users that Facebook collects their medical information in violation of medical websites' privacy policies and HIPAA.

V. CLASS ACTION ALLEGATIONS

235. This putative class action is brought pursuant to Federal Rules of Civil Procedure 23(b)(2) and 23(b)(3). The Plaintiffs bring this action on behalf of themselves and all similarly situated individuals as representatives of a class and subclasses defined as follows:

> **Facebook Medical Tracking Class:** All registered users of Facebook who communicated with medical organizations and providers through their web-browsers and who did not affirmatively consent to the release of those communications to Facebook.
>
> **Facebook Medical Direct Marketing Class:** All registered users of Facebook who communicated with medical organizations and providers through their web-browsers and who did not affirmatively consent to the release of those communications to Facebook and who were placed into advertising interest categories by Facebook based on that information for direct marketing purposes.
>
> **Cancer.org Subclass**: All registered users of Facebook who communicated with the American Cancer Society through their web-browsers via the website Cancer.org and who did not affirmatively consent to the release of those communications to Facebook.
>
> **Cancer.net Subclass:** All registered users of Facebook who communicated with the American Society of Clinical Oncology through their web-browsers via the website Cancer.net and who did not affirmatively consent to the release of those communications to Facebook.
>
> **Melanoma.org Subclass:** All registered users of Facebook who communicated with the Melanoma Research Foundation through their web-browsers via the website Melanoma.org and who did not affirmatively consent to the release of those communications to Facebook.
>
> **Adventist Subclass** – All registered users of Facebook who communicated with Adventist Health System through their web-browsers via the websites ShawneeMission.org, keepingyouwell.com, ctmc.org, chippewavalleyhospital.com, gordonhospital.com, manchestermemorial.com, mplex.org, porterhospital.org, takoma.org, texashealthhugeley.org, and texashealth.org and who did not affirmatively consent to the release of those communications to Facebook.
>
> **BJC Subclass** – All registered users of Facebook who communicated with BJC Healthcare through their web-browser via the websites BarnesJewish.org and BooneHospital.com, and who did not affirmatively consent to the release of those communications to Facebook.
>
> **Cleveland Clinic Subclass** – All registered users of Facebook who communicated with the Cleveland Clinic through their web-browser via the website

ClevelandClinic.org and who did not affirmatively consent to the release of those communications to Facebook.

MD Anderson Subclass – All registered users of Facebook who communicated with the University of Texas MD Anderson Cancer Center through their web-browser via the website MDAnderson.org and who did not affirmatively consent to the release of those communications to Facebook.

236. Plaintiff Winston Smith meets the requirements of both Facebook classes and the Cancer.org, Cancer.net, Melanoma.org and MD Anderson subclasses.

237. Plaintiff Jane Doe meets the requirements of the Facebook classes and the Adventist subclass.

238. Plaintiff Jane Doe II meets the requirements of the Facebook classes and the BJC and Cleveland Clinic subclasses.

239. The particular members of the proposed Classes are capable of being described without managerial or administrative difficulties. The members of the Classes are readily identifiable from the information and records in the possession or control of the Defendants.

240. The members of the Classes are so numerous that individual joinder of all members is impractical. This allegation is based upon information and belief that Defendants disclosed to and Facebook tracked and intercepted the health and cancer-related Internet search and browsing communications of millions of users.

241. There are questions of law and fact common to the Classes that predominate over any questions affecting only individual members of the Classes or Subclasses, and, in fact, the wrongs suffered and remedies sought by the Plaintiffs and other members of the Classes and Subclasses are premised upon an unlawful scheme participated in by each of the Defendants. The principal common issues include, but are not limited to, the following:

a. The extent to which the health care websites disclosed Plaintiffs' personally-identifiable cancer and other health information to Defendant Facebook;

b. The extent to which the disclosures and interceptions violated the privacy policies of the health care websites and Facebook.com;

c. Whether Defendants are liable to Plaintiffs under the federal Wiretap Act;

d. Whether Defendants are liable to Plaintiffs for Intrusion Upon Seclusion;

e. Whether Defendants are liable to Plaintiffs for violation of the California Invasion of Privacy Act, Cal. Pen. Code § 631, et. seq.;

f. Whether Defendants are liable to Plaintiffs under California's constitutional cause-of-action for invasion of privacy;

g. Whether Defendants are liable to Plaintiffs for negligence per se as a result of Defendants' violations of the Wiretap Act, the Pen Register Act, the Computer Fraud and Abuse Act, the California Invasion of Privacy Act, and for Facebook only, Cal. Civ. Code §1798.91, relating to disclosures required for non-health care businesses to use, share, or disclose medical information for purposes of direct marketing;

h. Whether the health care Defendants are liable to Plaintiffs for the negligent disclosure of confidential information;

i. Whether the health care Defendants are liable to Plaintiffs for breach of a fiduciary duties of confidentiality;

j. Whether Defendant Facebook is liable to Plaintiffs for breach of the duty of good faith and fair dealing;

k. Whether Defendant Facebook is liable to Plaintiffs for quantum meruit;

l. The nature and extent of all statutory penalties or damages for which the Defendants are liable to the Class members;

m. Whether the conduct complained of herein should be enjoined; and

n. Whether punitive damages are appropriate.

242. The common issues predominate over any individualized issues such that the putative classes are sufficiently cohesive to warrant adjudication by representation.

243. Plaintiffs' claims are typical of those of the members of the Classes and based on the same legal and factual theories.

244. Class treatment is superior in that the fairness and efficiency of class procedure in

this action significantly outweighs any alternative methods of adjudication. In the absence of class treatment, duplicative evidence of Defendants' alleged violations would have to be provided in thousands of individual lawsuits. Moreover, class certification would further the policy underlying Rule 23 by aggregating class members possessing relatively small individual claims, thus overcoming the problem that small recoveries do not incentivize plaintiffs to sue individually.

245. The Plaintiffs will fairly and adequately represent and protect the interests of the members of the Class. The Plaintiffs have suffered injury in their own capacity from the practices complained of and are ready, willing, and able to serve as Class representatives. Moreover, Plaintiffs' counsel is experienced in handling class actions and actions involving unlawful commercial practices, including such unlawful practices on the Internet. Neither the Plaintiffs nor their counsel has any interest that might cause them not to vigorously pursue this action. The Plaintiffs' interests coincide with, and are not antagonistic to, those of the Class members they seek to represent.

246. Certification of a class under Federal Rule of Civil Procedure 23(b)(2) is appropriate because the Defendants have acted on grounds that apply generally to the Class such that final injunctive relief is appropriate respecting the Class and Subclass as a whole.

247. Certification of a class under Federal Rule of Civil Procedure 23(b)(3) is appropriate in that the Plaintiffs and the Class Members seek monetary damages, common questions predominate over any individual questions, and a class action is superior for the fair and efficient adjudication of this controversy. A class action will cause an orderly and expeditious administration of Class members' claims and economies of time, effort, and expense will be fostered and uniformity of decisions will be ensured. Moreover, the individual members of the Class are likely to be unaware of their rights and not in a position (either financially or through experience) to commence individual litigation against these Defendants.

248. Alternatively, certification of a plaintiff class under Federal Rule of Civil Procedure 23(b)(1) is appropriate in that inconsistent or varying adjudications with respect to individual members of the Class would establish incompatible standards of conduct for the Defendants or adjudications with respect to individual members of the Class as a practical matter would be

dispositive of the interests of the other members not parties to the adjudication or would substantially impair or impede their ability to protect their interests.

VI. CAUSES OF ACTION

COUNT I – WIRETAP ACT

(Against All Defendants)

249. Plaintiffs hereby incorporate all other paragraphs as if fully stated herein.

250. The Wiretap Act prohibits the intentional interception of the contents of any wire, oral, or electronic communication through the use of a device.

251. The Wiretap Act protects both the sending and receipt of communications.

252. The Wiretap Act provides a private right of action for any person whose wire, oral, or electronic communication (whether being sent or received) is intercepted. 18 U.S.C. § 2520(a).

253. Facebook's actions in intercepting, tracking, and acquiring user communications at medical websites in violation of those websites' privacy policies, and, for covered entities, HIPAA, was intentional in that Facebook purposefully designed its code to track, intercept, and acquire user communications connected to personally-identifiable information.

254. Facebook's tracking involved the acquisition of information relating to the substance, purport, or meaning of communications that Plaintiffs were in the process of sending to and receiving from the medical websites. Facebook's acquisition of the information was contemporaneous to the sending and receipt of said communications and Facebook, in fact, acquired the copy of the contents of the communications before the communications between the plaintiffs and the medical websites were completed.

255. Facebook's acquisition of the plaintiffs' communications to and from the medical websites was accomplished through a separate channel than the path of the actual communication between the users and the medical websites.

256. Facebook's acquisitions included "contents" of electronic communications that Plaintiffs sent to and received from the medical websites in the form of (1) GET requests which included URL file paths, (2) detailed URL requests, and (3) search queries which Plaintiffs sent to the medical websites and for which Plaintiffs received communications from the medical websites.

For example, with the referer URL

http://www2.mdanderson.org/cancerwise/2012/06/metastatic-melanoma-a-wife-reflects-on-husbands-shocking-diagnosis.html

the phrase "metastatic melanoma a wife reflects on husbands shocking diagnosis" contains information relating to the substance, purport, and meaning of the communications between the user and MD Anderson.

257. The transmission of data between Plaintiffs and the medical websites that Facebook tracked, intercepted, and acquired without authorization involves the "transfer of signs, signals, writing, … data [and] intelligence of [some] nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic, or photooptical system that affects interstate commerce[,] and were therefore "electronic communications" within the meaning of 18 U.S.C. § 2510(12).

258. For each communication sequence at issue, the Plaintiffs began the communications to the medical websites via one of three methods:

a. By directly typing the exact URL into their web-browser, then taking the affirmative action of either hitting the Enter button or clicking on their mouse to send the communication;

b. By conducting a search either at the medical website or some other website seeking information relating to a topic and then clicking on a hyperlink with text indicating that clicking on the link will send a communication to the medical website seeking information on the topic and for which the recipient website will send a return communication with information about the topic requested; or

c. By clicking on a hyperlink on a different webpage where the hyperlink indicates that clicking on it will send a communication to the recipient medical website linked to the information that the Plaintiff is seeking and that is referenced in the hyper-link.

259. Each method of sending a communication on their web-browser involves a choice by the plaintiff Internet user and Class Member to send a communication relating to the topic.

Users do not randomly send or receive these communications, but instead make them through conscious communications and requests for specific information. Whether an Internet user types the full-string URL into their browser or uses the technological short-cut of left-clicking on a hyperlink with their mouse, the intent and effect is the same: they are sending a communication and taking an action which causes the "transfer" of signs, signals, data, and other intelligence to the health care Defendants from which they are also receiving communications in return.

260. The words and other data contained within URL file paths are similarly not random but instead are the result of conscious choices and communications made by the health care Defendants.

261. The following constitute "devices" within the meaning of 18 U.S.C. §2510(5):

a. The cookies and other tools the Facebook used to track the Plaintiffs' communications while they were communication with the medical websites;

b. The Plaintiffs' web-browsers;

c. The Plaintiffs' computing devices;

d. Facebook's web-servers;

e. The web-servers of the medical websites from which the Facebook acquired the Plaintiffs' communications;

f. The computer code deployed by Facebook to effectuate its acquisition of the Plaintiffs' communications with the medical websites; and

g. The plan Facebook carried out to effectuate the tracking and interception of user communications while on medical websites.

262. As illustrated above, "the" communications between the Plaintiffs and the medical websites were simultaneous, but separate from, the channel through which Facebook acquired the content of those communications.

263. Facebook intentionally acquired the contents of Plaintiffs' electronic communications with every medical website specifically mentioned in this Complaint and hundreds of others attached to personally-identifiable information through the process described

above.

264. Each website of a health care Defendant in this case has control of its own website:

a. Defendant ACS controls Cancer.org;

b. Defendant ASCO controls Cancer.net;

c. Defendant MRF controls Melanoma.org;

d. Defendant Adventist controls ShawneeMission.org and its other websites;

e. Defendant BJC controls BarnesJewish.org;

f. Defendant Cleveland Clinic controls ClevelandClinic.org; and

g. Defendant MDAnderson controls MDAnderson.org.

265. The health care Defendants each, respectively, placed code on their websites and web-pages which facilitated the disclosure, tracking, interception, and acquisition of the Plaintiffs' communications with the medical websites by Facebook through the process described in this Complaint.

266. The disclosure, tracking, interception, and acquisition of the Plaintiffs' health-related communications to and from the medical websites by Facebook was not authorized by the Plaintiffs.

a. The disclosure, tracking, and interception was done without their knowledge;

b. The disclosure, tracking, and interception was done without their express or implied consent, despite the fact that sensitive medical information, including communications, are protected by state and federal laws (including HIPAA) which explicitly require affirmative, detailed written consent before such information can be disclosed to or tracked by a third-party;

c. The disclosure, tracking, and interception was further done without their express or implied consent and was, in fact, contrary to the privacy policies of the medical websites with which they were sending and receiving medical communications;

d. The disclosure, tracking, and interception was further done without their express or implied consent because Facebook failed to provide users with any notice that it tracked their communications on medical websites in violation of those websites privacy policies and HIPAA, or that it tracked communications with medical websites for purposes of placing its users into categories for purposes of direct marketing to users with sensitive medical conditions and interests;

e. In addition to the facts set forth above, Facebook lacked the Plaintiffs' express consent as a matter of law because they did not make any disclosure that they tracked sensitive medical information. Nor did they obtain consent for such disclosure consistent with HIPAA or California law regarding medical privacy;

f. In addition to the facts set forth above, Facebook lacked the Plaintiffs' express and implied consent as a matter of law because medical privacy enjoys greater protection than other general Internet privacy and the Facebook and the health care Defendants failed to make any disclosures related to the interception of medical communications; and

g. In addition to the facts set forth above, Facebook lacked the Plaintiffs' express and implied consent as a matter of law because Facebook's tracking on the health care Defendants' websites violated the privacy policies of those websites, all of which were either scanned or available to be scanned by Facebook's web-crawler and, accordingly, Facebook had either actual or constructive knowledge that it was intercepting communications in violation of those privacy policies.

267. Facebook's scheme involved the contemporaneous acquisition of the contents of communications Plaintiffs were in the process of making to and receiving from the health care Defendants. As detailed above, Facebook acquired the content of communications within milliseconds of the Plaintiffs' GET requests to the medical websites, in such a fashion that the

Plaintiffs would have no reason to suspect Facebook acquired the communications, and before the communications between the Plaintiffs and the respective medical websites had been completed.

268. The interceptions included the "contents" of such electronic communications in the form of detailed URLs requested, search queries, and 'GET' requests made by Plaintiffs.

269. For the lead-Plaintiffs, these "contents" included the following communications which contained information relating to the substance, purport, or meaning of the named Plaintiffs' communications:

a. For Defendant ACS, the following contain information relating to the "substance, purport, or meaning" of a communication:

- Cancer – Treatment – Support Program Services – Index
- Cancer – Finding and Paying for Treatment – Understanding Health Insurance – Health Insurance and Financial Assistance for the Cancer Patient—Health Insurance and Financial Assistance TOC
- Cancer – Treatment – Finding and Paying for Treatment – Understanding Health Insurance – Prescription Drug Assistance Programs – Prescription Drug Assistance Programs – TOC
- Lung Cancer – Small Cell – Detailed Guide – Small Cell Lung Cancer After Lifestyle Changes

b. For Defendant ASCO, the following contain information relating to the "substance, purport, or meaning" of a communication:

i. Cancer – Navigating Cancer Care – Financial Consideration – Financial Resources

ii. Cancer – Cancer Types – Melanoma – Treatment Options

iii. Cancer – Navigating Cancer Care – Diagnosing Cancer – Tests and Procedures – Positron Emission Tomography PET Scan

c. For Defendant MRF, the following contain information relating to the "substance, purport, or meaning" of a communication: Melanoma – Find Support – Patient Community – MPIP Melanoma

d. For Defendant Adventist, the following contain information relating to the "substance, purport, or meaning" of a communication:

i. Shawnee Mission – Health Services – Center for Pain Medicine

ii. Shawnee Mission – Orthopaedic Spine Center

iii. Shawnee Mission – Find a Doctor – Scott E. Ashcraft MD

e. For Defendant BJC, the following contain information relating to the "substance, purport, or meaning" of a communication:

i. Barnes Jewish – Physicians – Details Physician 1033041

ii. Barnes Jewish – Physicians – Details Physician 1027051

f. For Defendant Cleveland Clinic, the following contains information relating to the "substance, purport, or meaning" of a communication: Cleveland Clinic – Search – Results – Q – Intestine Transplant

g. For Defendant MD Anderson, the following contains information relating to the "substance, purport, or meaning" of a communication: MD Anderson – Cancer Wise – Metastatic Melanoma – A Wife Reflects on Husbands Shocking Diagnosis

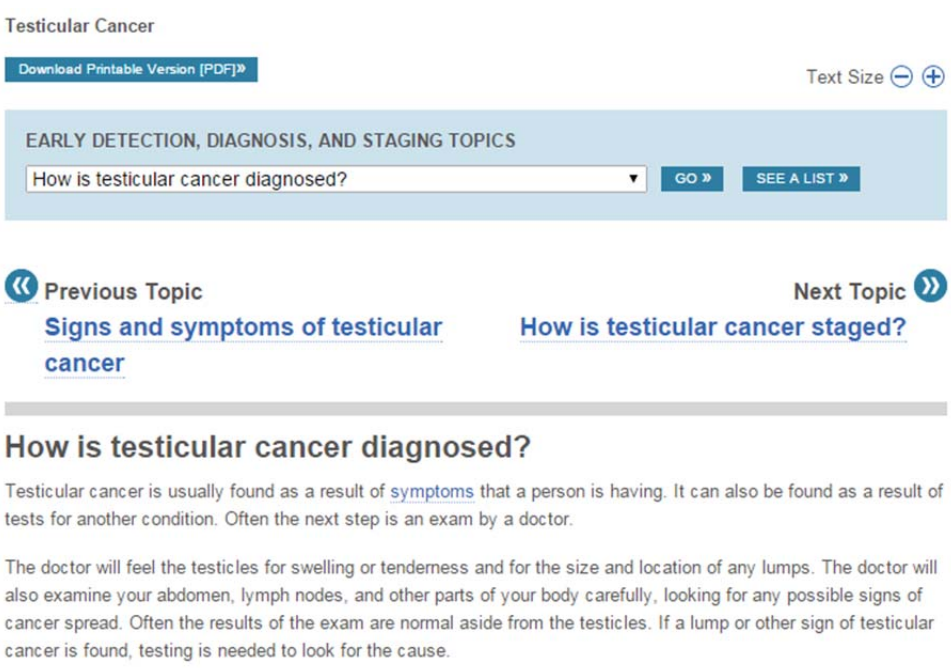
270. In addition to acquiring "content" of the plaintiffs' communications to the health care Defendants, Facebook also intercepted "content" of the communications Plaintiffs received in return from the health care Defendants. For example, the GET request for the Cancer.org webpage: http://www.cancer.org/cancer/testicularcancer/detailedguide/testicular-cancer-diagnosis, returns a communication from Cancer.org with a nearly 2,000 word essay on how testicular cancer is diagnosed. The following is a partial screenshot of the communication Cancer.org sent in response to such a GET request. It includes approximately 1/16th of the total communication from Cancer.org in response to the GET request:

/ / /

/ / /

/ / /

/ / /



271. GET requests are electronic communications because they involves a "transfer of signs, signals, writing, … data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic or photooptical system that affects interstate … commerce."

272. Every URL detailed in this Complaint was included with a GET request.

273. The Plaintiffs' particular GET requests were communications.

274. Web-server and website responses to GET requests are communications.

275. The health care Defendants' responses to Plaintiffs' GET requests in this case were communications.

276. A substantially similar or identical process was carried out for communications sent to and received from the other Defendants' medical websites.

277. The consent of a party to a communication is an affirmative defense under the Wiretap Act which must be plead and proven by a defendant claiming the exception.

278. Though each health care Defendant intentionally placed or allowed to be placed computer code on their websites which permitted Facebook to acquire the Plaintiffs' health-related Internet communications in violation of each health care Defendants' privacy policy, Plaintiffs are without knowledge whether Facebook's interceptions were indeed carried out with the knowledge

and consent of the health care Defendants.

279. Plaintiffs are without knowledge of the absence or existence of private communications or agreements between Facebook and each health care Defendant which may evince the express consent to such tracking by the health care Defendants.

280. Facebook's public notice to potential developers and website owners is deficient with respect to its plan to track the personally-identifiable information of Facebook users and intercept communications to and from websites which place Facebook code on their webpages.

281. Facebook's page explaining its "Like Button for the Web" to Developers does not disclose that installing a Like button on a webpage permits Facebook to track communications of its individually-identifiable users with the webpage installing the Like button whether or not the user actually clicks on the Like button.[30] *See* Exhibit D for Facebook Developer Pages.

282. Facebook's "Social Plugins FAQs" page for developers does not disclose that installing a Like button permits Facebook to track communications of its individually-identifiable users whether the user clicks on the Like button or not.[31]

283. To plaintiffs' knowledge, Facebook does not disclose its tracking or interception of communications via the Like button anywhere on its Developer platform.

284. To plaintiffs' knowledge, Facebook does not disclose its tracking or interception of communications via the Share button or other graphics on its Developer platform.

285. Facebook has actual or constructive knowledge of the content of the Privacy Policy of each webpage which includes social plug-ins or links to Facebook.

286. In its "Social Plugins FAQs," Facebook informs that it "scrape[s]" developer "page[s] every 30 days."[32]

287. Facebook's web-crawler scrapes the Privacy Policies of websites hosting social plug-ins.

288. The privacy policies of the health care Defendants explicitly promise not to

[30] See https://developers.facebook.com/docs/plugins/like-button.
[31] See https://developers.facebook.com/docs/plugins/faqs.
[32] See https://developers.facebook.com/docs/plugins/faqs/#scraperinfo.

disclose personally-identifiable information to third-parties like Facebook.

289. Despite Facebook's constructive and actual knowledge of the health care Defendants' privacy policies, they continued to track and intercept user communications with those websites in violation of the medical website privacy policies.

290. Facebook's constructive and actual knowledge that their respective interceptions were violating the privacy policies of the health care Defendants put it on notice that those medical websites neither knew nor consented to Facebook's tracking and interceptions of communications on those websites.

291. In the event discovery reveals any particular health care Defendant lacked knowledge or did not consent to the tracking and interceptions of health-related Internet communications, Facebook is liable both to the particular Plaintiff subclass and the non-consenting health care Defendant.

292. Upon information and belief, the health care Defendants lack financial or any other significant incentive to violate their own privacy policies and flout HIPAA for any benefit gained by placing Facebook's computer code on their respective medical web-pages. Discovery is necessary to determine the extent of their knowledge of and consent (or lack thereof) to Defendant Facebook's tracking and interceptions.

293. In the event discovery reveals any particular health care Defendant did consent to interceptions by Facebook, Plaintiffs hereby allege the interception was accomplished through a scheme by which each consenting Defendant and Facebook committed criminal and tortious acts in violation of the laws of the United States and all 50 states. In particular, Defendants' scheme:

a. Violated the Computer Fraud and Abuse Act and corresponding computer crime laws in all 50 states because Defendants knowingly placed or facilitated the placement of onto Plaintiffs' computing devices third-party cookies which tracked Plaintiffs' personally-identifiable and sensitive medical information without their consent, thereby intentionally exceeding authorized access to and obtaining information from the Plaintiffs' computers. Intentionally exceeding authorization and obtaining information

from a computer used in interstate commerce violates the Computer Fraud and Abuse Act, 18 U.S.C. § 1030(a)(2)(C), and corresponding computer crime laws of all 50 states;

b. Constituted a tortious intrusion upon seclusion as alleged herein;

c. Violated the criminal provisions of the California Invasion of Privacy Act as alleged herein;

d. Involved criminal and civil violations of HIPAA;

e. Constituted negligence per se;

f. Constituted the negligent disclosure of confidential information; and

g. Constituted a breach of fiduciary duties of confidentiality.

294. As a result of the above violations and pursuant to 18 U.S.C. § 2520, the Court may assess statutory damages to Plaintiffs and the Class in the sum of the greater of $100 for each day each Class Member's electronic communications were intercepted, disclosed, or used, or $10,000 per violation, whichever is greater; injunctive and declaratory relief, punitive damages in an amount to be determined by a jury, but sufficient to prevent the same or similar conduct by Defendants in the future, and a reasonable attorney's fee and other litigation costs reasonably incurred.

COUNT II – INTRUSION UPON SECLUSION

(Against All Defendants)

295. Plaintiffs hereby incorporate all other paragraphs as if fully stated herein.

296. In carrying out the scheme to disclose, divulge, track, and intercept the Plaintiffs' personal information combined with medical information and communications without the consent of the Plaintiffs, Defendants intentionally intruded upon the Plaintiffs' solitude or seclusion in that they disclosed and tracked highly-confidential, personally-identifiable medical information and communications from the privacy of the Plaintiffs' homes and computing devices.

297. The Plaintiffs' medical communications constitute private conversations and matters.

298. The Plaintiffs' medical communications with the health care Defendants were

promised to be kept private by the privacy policies of the health care Defendants.

299. By law, the Plaintiffs' medical communications with covered entities under HIPAA must remain private unless the Plaintiffs provide their express written consent to a disclosure on a form consistent with the requirements of HIPAA.

300. The Plaintiffs had no knowledge of and did not expressly or impliedly consent to:

a. The health care Defendants' disclosures of their medical communications to Facebook;

b. Facebook's acquisition of their communications with the health care Defendants; or

c. Facebook's taking of their personal information and medical information for purposes of direct marketing by placing them into medical categories for sale to advertisers.

301. Defendants' intentional intrusion on the Plaintiffs' solitude or seclusion is highly offensive to a reasonable person in that they violated federal and state criminal and civil statutes designed to protect individual privacy. Specifically, Defendants' conduct violated:

a. The Wiretap Act as alleged herein;

b. The Pen Register Act, 18 U.S.C. §3121, which prohibits the non-consensual installation or use of a pen register or trap and trace device. A "pen register" is "a device or process which records or decodes dialing, routing, addressing, or signaling information transmitted by an instrument or facility from which a wire or electronic communication is transmitted, provided, however, that such information shall not include the contents of any communication." The cookies at issue in this case intercept both "content" and "dialing, routing, addressing, and signaling" information and therefore fall under the Pen Register Act. A "trap and trace device" is "a device or process which captures the incoming electronic or other impulses which identify the originating number or other dialing, routing, addressing, and signaling information reasonably likely to identify the source of a wire or

electronic communication." The cookies at issue in this case also work as "trap and trace" devices because, in addition to capturing content, they also capture impulses identifying the originating number and other dialing, routing, addressing, and signaling information. These pen registers and trap-and-trace devices were installed and used by Facebook and the health care Defendants without Plaintiffs' knowledge or consent;

c. The Computer Fraud and Abuse Act and corresponding computer crime laws in all 50 states because Defendants' knowingly placed or facilitated the placement of third-party cookies on the computing devices of the Plaintiffs' which tracked personally-identifiable information without the Plaintiffs' consent, thereby intentionally exceeding authorized access to the Plaintiffs' computers and obtaining information from their computers. Intentional access to a computer which exceeds authorization and results in the obtaining of information from a computer used in interstate commerce violates the Computer Fraud and Abuse Act, 18 U.S.C. § 1030(a)(2)(C), and corresponding computer crime laws of all 50 states;

d. The California Invasion of Privacy Act, Cal. Pen. Code § 631;

e. HIPAA; and

f. For Facebook, violated California Civ. Code §1798.91, which provides that "[a] business may not request in writing medical information directly from an individual regardless of whether the information pertains to the individual or not, and use, share or otherwise disclose that information for direct marketing purposes" unless it first "disclose[s] in a clear and conspicuous manner that it is obtaining the information to market or advertise products, goods, or services to the individual" and "obtain[s] the written consent of the individual to whom the information pertains … to permit his or her medical information to be used or shared to market or advertise products, goods, or services to the individual."

302. In addition to engaging in activity which comprises a criminal offense under federal law and all 50 states, the unauthorized disclosure and tracking of the Plaintiffs' highly-confidential and personally-identifiable cancer and other medical-related communications and information is, in and of itself, highly offensive to reasonable people.

303. Defendants' unauthorized disclosures and tracking were perpetrated on millions of unsuspecting Americans, which is also highly offensive to a reasonable persons.

304. Plaintiffs sustained economic damage through Defendants' intrusion upon their seclusion by way of economic loss associated with the medical information taken without their consent and general damages for the Defendants' invasion into the Plaintiffs' zone of privacy for which damages are available without proof of pecuniary loss or physical harm. Under the common law tort of intrusion upon seclusion, general damages are presumed: a monetary award calculated without reference to specific harm, but to be calculated by a jury. Plaintiffs also seek compensation for any revenues or other benefits the Defendants derived from the invasion of Plaintiffs' right to privacy. Finally, Plaintiffs seek punitive damages in this claim in an amount to be determined by a jury.

COUNT III – CALIFORNIA INVASION OF PRIVACY ACT

(Against All Defendants)

305. Plaintiffs hereby incorporate all other paragraphs as if fully stated herein.

306. Defendant Facebook:

a. Is headquartered in California;

b. Directs its Internet tracking activities from California;

c. Receives tracked Internet communications in California;

d. Includes a binding Terms of Use adopting California law to govern all disputes with their members; and

e. Upon information and belief, requires developers to agree to its Terms of Use adopting California law to govern disputes with developers and websites utilizing Facebook code.

307. Plaintiffs are without knowledge as to whether the health care Defendants had

knowledge of and consented to Facebook's acquisition of the contents of Internet communications made between the Plaintiffs and the health care Defendants. In the event that any health care Defendant had knowledge and consented, it subjected itself to California law by knowingly disclosing Plaintiffs' communications to Facebook, which is headquartered in, operates out of, and adopts California law to govern disputes involving their business practices.

308. California Penal Code § 631(a) provides, in pertinent part:

> Any person who … willfully and *without the consent of all parties* to the communication, or in any unauthorized manner, reads, or attempts to read, or to learn the contents or meaning of any message, report, or communication while the same is in transit or passing over any wire, line, or cable, or is being sent from, or received at any place within this state; or who uses, or attempts to use, in any manner, or for any purpose, or to communicate in any way, any information so obtained, or who aids, agrees with, employs, or conspires with any person or persons to lawfully do, or permit, or cause to be done any of the acts or things mentioned above in this section, is punishable by a fine not exceeding two thousand five hundred dollars.

309. In addition, California Penal Code § 632 provides, in pertinent part:

> Every person who, intentionally and without the consent of all parties to a confidential communication, by means of any … recording device, ... records the confidential communication … shall be punished by a fine not exceeding [$2,500].

310. California Penal Code § 637.2 creates a civil cause of action for any person whose rights have been violated under § 631 or 632 and provides for statutory damages for the greater of $5,000 or three times the amount of actual damages, as well as injunctive relief.

311. The California Invasion of Privacy Act in § 631(a) has been interpreted to be identical to its federal Wiretap counterpart with one key difference – to avoid liability under CIPA, an interceptor must obtain "the consent of all parties to the communication."

312. Plaintiffs' communications with the health care Defendants are communications covered by §631(a).

313. Plaintiffs' communications with the health care Defendants are confidential because they were carried on in circumstances reasonably indicating to the Plaintiffs that they would be confined to the parties thereto.

314. Plaintiffs' communications with the health care Defendants included "content" as

defined under § 631(a) and the federal Wiretap Act in that GET requests, search queries, and full-string URLs containing file paths include information "relating to the substance, purport, or meaning" of communications.

315. Defendants' disclosures, interceptions, acquisitions and tracking were accomplished while Plaintiffs' communications were in transit, being sent from, or being received at places in California.

316. Defendants' disclosures, interceptions, acquisitions, and tracking were done without the Plaintiffs' knowledge or consent and in direct contravention of the Defendants' Privacy Policies and federal and state laws on medical privacy.

317. Plaintiffs are without knowledge of whether the health care Defendants gave either their express or implied consent for Facebook to intercept medical communications the health care Defendants sent to and received from the Plaintiffs. Upon information and belief, the health care Defendants lacked sufficient incentives to reasonably conclude in the absence of discovery that they expressly or impliedly consented to Facebook's conduct. To Plaintiffs' knowledge, Facebook did not publicly disclose on its developer pages that its code would result in Facebook's tracking of communications between the owners of the webpages on which the code was placed and Internet users. Further, Facebook had actual and constructive knowledge of the health care Defendants' privacy policies and their status as "covered entities" under HIPAA through their website names and the fact that their web-pages were either scraped or available to be scraped by Facebook's web-crawlers. Discovery is necessary to determine if there exist any private communications between Facebook and the health care Defendants relating to consent. However, to the extent no communications between Facebook and the health care Defendants are produced showing either express or implied consent, the health care Defendants each have their own cause-of-action under CIPA and the federal Wiretap Act against Facebook.

318. Defendants additionally used and communicated such information to their benefit and to the detriment of Plaintiffs.

319. To the extent the health care Defendants were aware of and consented to Facebook's acquisition of the contents of the Plaintiffs' communications with the health care

Defendants, they are liable under §631(a) for "aid[ing], agree[ing] with, employ[ing], or conspir[ing] with" Facebook to "unlawfully do, or permit, or cause to be done" actions in violation of § 631(a).

320. Facebook is not a party to the communications between the Plaintiffs and the health care Defendants. However, in the alternative, if the Court deems Facebook to be a party to the communications as a matter of law, Facebook remains liable under Cal. Pen. Code § 632(a).

321. Pursuant to §637.2, persons whose rights are violated under the California Invasion of Privacy Act "may bring an action against the person who committed the violation for the greater of … "$5,000" or "[t]hree times the amount of actual damages, if any, sustained by the plaintiff." The California Act is clear that it "is not a necessary prerequisite to an action pursuant to this section that the Plaintiff has suffered, or be threatened with, actual damages."

COUNT IV – CALIFORNIA CONSTITUTIONAL INVASION OF PRIVACY

(Against All Defendants)

322. Plaintiffs hereby incorporate all other paragraphs as if fully stated herein.

323. Art. I, sec. 1 of the California constitution declares that "[a]ll people are by nature free and independent and have inalienable rights[]" which include the right to "privacy."

324. Art. I, sec. 1 of the California constitution creates a right of action against private as well as government entities that violate privacy rights in California where the plaintiffs have a legally protected privacy interest, a reasonable expectation of privacy, and the defendant's action constitutes a serious invasion of privacy.

325. Plaintiffs have several specific legally protected privacy interests in their sensitive, health-related Internet communications with the health care Defendants. These rights include:

a. The Wiretap Act as alleged herein;

b. The Pen Register Act, 18 U.S.C. §3121, which prohibits the non-consensual installation or use of a pen register or trap and trace device. A "pen register" is "a device or process which records or decodes dialing, routing, addressing, or signaling information transmitted by an instrument or facility from which a wire or electronic communication is transmitted, provided,

however, that such information shall not include the contents of any communication." The cookies at issue in this case intercept both "content" and "dialing, routing, addressing, and signaling" information and therefore fall under the Pen Register Act. A "trap and trace device" is "a device or process which captures the incoming electronic or other impulses which identify the originating number or other dialing, routing, addressing, and signaling information reasonably likely to identify the source of a wire or electronic communication." The cookies at issue in this case also work as "trap and trace" devices because, in addition to capturing content, they also capture impulses identifying the originating number and other dialing, routing, addressing, and signaling information. These pen registers and trap-and-trace devices were installed and used by Facebook and the health care Defendants without Plaintiffs' knowledge or consent;

c. The Computer Fraud and Abuse Act and corresponding computer crime laws in all 50 states because Defendants' knowingly placed or facilitated the placement of third-party cookies on the computing devices of the Plaintiffs which tracked personally-identifiable information without the Plaintiffs' consent, thereby intentionally exceeding authorized access to the Plaintiffs' computers and obtaining information from their computers. Intentional access to a computer which exceeds authorization and results in the obtaining of information from a computer used in interstate commerce violates the Computer Fraud and Abuse Act, 18 U.S.C. § 1030(a)(2)(C), and corresponding computer crime laws of all 50 states;

d. The California Invasion of Privacy Act;

e. HIPAA;

f. California Civ. Code §1798.91, which prohibits non-healthcare providers using, sharing, or otherwise disclosing individually identifiable information about a person's medical history, treatment, or diagnosis for purposes of

direct-marketing unless it (1) discloses in a clear and conspicuous manner it is obtaining the information to market or advertise products, good, and services, and (2) obtains written consent to permit their medical information to be used or shared to market or advertise products, goods, or services to the individual; and

g. The privacy policies of the health care Defendants in this case.

326. Plaintiffs have a reasonable expectation of privacy that Facebook would not acquire and the health care Defendants would not disclose their medical communications with the healthcare Defendants' websites and other websites of health care providers in that:

a. Facebook's acquisitions violate the Privacy Policies of those websites;

b. Facebook fails to disclose that it tracks, intercepts, and acquires user communications in violation of other websites' privacy policies;

c. Facebook fails to disclose that it tracks, intercepts, and acquires communications on healthcare websites and the websites of healthcare providers;

d. Facebook fails to disclose its direct marketing activities pursuant to the requirements of Cal. Civ. Code §1798.91, yet maintains direct marketing lists of 255 million Facebook users in the United States grouped by sensitive medical categories and sells direct marketing access to those lists to advertisers; and

e. The actions of the health care Defendants and Facebook violate the federal and state criminal and civil laws set forth above, and it is reasonable for Plaintiffs to expect that health care Defendants and Facebook would not commit illegal acts against them.

327. Defendants' invasions of Plaintiffs' privacy interests constitute a serious invasion of privacy in that health-related communications and records are among the types of information Americans hold most secret and are, accordingly, protected by state and federal law.

328. Defendants' invasions of Plaintiffs' privacy interests constitute an egregious breach

of social norms.

329. Facebook lacks a legitimate business interest in tracking, intercepting, and acquiring sensitive medical communications. Any interest Facebook has in tracking, intercepting, and acquiring sensitive medical communications is outweighed by the Plaintiffs' rights to privacy, as evidence by social norms and the federal and state criminal and civil statutes set forth above.

330. The health care Defendants lack legitimate business interests in disclosing sensitive medical communications to Facebook. Any interest the health care Defendants have in those disclosures is outweighed by the Plaintiffs' rights to privacy, as evidenced by social norms and the federal and state criminal and civil statutes set forth above.

331. Plaintiffs and the class members sustained damage through Defendants' invasion of their constitutional right to privacy under the California Constitution by way of economic loss associated with the medical information taken without their consent and general damages for the Defendants' invasion into the Plaintiffs' zone of privacy for which damages are available without proof of pecuniary loss or physical harm. Under the common law tort of intrusion upon seclusion, general damages are presumed: a monetary award calculated without reference to specific harm, but to be calculated by a jury. Plaintiffs seek compensation for any revenues or other benefits the medical website and/or Tracker Defendants derived from the invasion of Plaintiffs' constitutional rights. Finally, Plaintiffs seek punitive damages in this claim in an amount to be determined by a jury.

COUNT V – NEGLIGENCE PER SE

(Against All Defendants)

332. Plaintiffs hereby incorporate all other paragraphs as if fully stated herein.

333. Defendants' conduct violated several criminal and civil laws of the United States and individual states, including:

a. The Wiretap Act as alleged herein;

b. The Pen Register Act, 18 U.S.C. §3121, which prohibits the non-consensual installation or use of a pen register or trap and trace device. A "pen register" is "a device or process which records or decodes dialing, routing,

addressing, or signaling information transmitted by an instrument or facility from which a wire or electronic communication is transmitted, provided, however, that such information shall not include the contents of any communication." The cookies at issue in this case intercept both "content" and "dialing, routing, addressing, and signaling" information and therefore fall under the Pen Register Act. A "trap and trace device" is "a device or process which captures the incoming electronic or other impulses which identify the originating number or other dialing, routing, addressing, and signaling information reasonably likely to identify the source of a wire or electronic communication." The cookies at issue in this case also work as "trap and trace" devices because, in addition to capturing content, they also capture impulses identifying the originating number and other dialing, routing, addressing, and signaling information. These pen registers and trap-and-trace devices were installed and used by Facebook and the health care Defendants without Plaintiffs' knowledge or consent;

c. The Computer Fraud and Abuse Act and corresponding computer crime laws in all 50 states because Defendants' knowingly placed or facilitated the placement of third-party cookies on the computing devices of the Plaintiffs' which tracked personally-identifiable information without the Plaintiffs' consent, thereby intentionally exceeding authorized access to the Plaintiffs' computers and obtaining information from their computers. Intentional access to a computer which exceeds authorization and results in the obtaining of information from a computer used in interstate commerce violates the Computer Fraud and Abuse Act, 18 U.S.C. § 1030(a)(2)(C), and corresponding computer crime laws of all 50 states;

d. The California Invasion of Privacy Act;

e. HIPAA; and

f. For Facebook, violated California Civ. Code §1798.91, which prohibits

non-healthcare providers using, sharing, or otherwise disclosing individually identifiable information about a person's medical history, treatment, or diagnosis for purposes of direct-marketing unless it (1) discloses in a clear and conspicuous manner it is obtaining the information to market or advertise products, good, and services, and (2) obtains written consent to permit their medical information to be used or shared to market or advertise products, goods, or services to the individual.

334. The Wiretap Act, Pen Register Act, Computer Fraud and Abuse Act and its corresponding 50 state analog statutes, impose criminal penalties on violators.

335. These statutes and rules are designed to protect the Internet privacy and medical privacy of American citizens.

336. The Plaintiffs are members of the protected classes of the above-cited statutes.

337. As a result of Defendants' violations of these statutes, Plaintiffs and the class members were harmed by having their sensitive medical-information disclosed, tracked, and intercepted without their knowledge or consent. In addition, they were harmed by violation of Cal. Civ. Code §1798.91 through Facebook's use of their personally-identifiable medical information for direct marketing purposes after the information was collected directly from Plaintiffs without the consent required by law.

COUNT VI – NEGLIGENT DISCLOSURE OF CONFIDENTIAL INFORMATION

(Against All Health Care Defendants)

338. Plaintiffs hereby incorporate all other paragraphs as if fully stated herein.

339. The health care Defendants had a duty to keep Plaintiffs' medical communications on the Internet with them confidential. This duty arises from:

a. For the Defendants that are "covered entities" under HIPAA, from their status as health-care providers and federal law;

b. For all health care Defendants, from their privacy policies promising users that they would not share or disclose their users' medical communications to third-parties.

340. By designing their websites in a fashion that facilitated the disclosure to, tracking, and interception of Plaintiffs' medical communications by Facebook, the health care Defendants breached their duty of confidentiality.

341. The health care Defendants' website designs caused Plaintiffs' confidential medical communications to be divulged to Facebook without Plaintiffs' knowledge or consent.

342. As a result of the above-pleaded facts, Plaintiffs and the class members suffered damage in that what the Plaintiffs intended to remain private is no longer so, their personally-identifiable confidential medical communications and records were disclosed to, tracked, and intercepted by Facebook without their consent.

COUNT VII – BREACH OF FIDUCIARY DUTY OF CONFIDENTIALITY

(Against All Health Care Defendants)

343. Plaintiffs hereby incorporate all other paragraphs as if fully stated herein.

344. The health care Defendants that are covered entities under HIPAA have a fiduciary duty to maintain the confidentiality of medical communications.

345. All of the health care Defendants created a fiduciary duty through their privacy policies to maintain the confidentiality of medical communications and records from users of their websites.

346. The health care Defendants breached their fiduciary duties of confidentiality to the plaintiff classes by designing their websites such that the websites disclosed to and permitted Facebook to track the Plaintiffs' confidential medical communications and records.

347. As a result of the above-pleaded facts, Plaintiffs and the class members suffered damage in that what the Plaintiffs intended to remain private is no longer so, their personally-identifiable confidential medical communications and records were disclosed to, tracked, and intercepted by Facebook without their consent.

COUNT VIII – BREACH OF DUTY OF GOOD FAITH AND FAIR DEALING

(Against Facebook)

348. Plaintiffs hereby incorporate all other paragraphs as if fully stated herein.

349. Defendant Facebook:

a. Is headquartered in California;

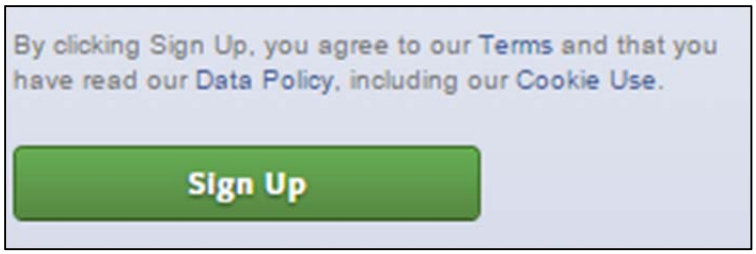
b. Directs Internet tracking activities from California;

c. Receives tracked Internet communications in California; and

d. Includes a Terms of Use adopting California law to govern all disputes with their members.

350. Every contract imposes upon each party a duty of good faith and fair dealing in its performance and enforcement.

351. Defendant Facebook and its users enter into a binding contract upon the user signing-up for the service by clicking on the "Signup" button located directly below a sentence informing the user, "By clicking Sign Up, you agree to our Terms and that you have read our Data Policy, including our Cookie Use."



352. Facebook users pay for Facebook's services with their personal information. Facebook's users exchange something of value – access to their personal information – for Facebook's services and Facebook's promise to safeguard that personal information and to act in a manner that is reasonable, consistent with the spirit of the bargain made, and does not abuse Facebook's power to specify the terms of the contract.

353. In dealings between Facebook and its users, Facebook is invested with discretionary power affecting the rights of its users.

354. Facebook purports to respect and protect its users' privacy. Facebook's "Terms" document claims:

> Your privacy is very important to us. We designed our Data Policy to make important disclosures about how you can use Facebook to share with others and how we collect and can use your content and information. We encourage you to read the Data Policy, and to use it to help you make informed decisions.

355. Despite Facebook's pledge to "make important disclosures" to users so they can "make informed decisions," Facebook's Data Policy fails to inform users that it:

a. Tracks users and intercepts their communications with websites in violation of those websites' privacy policies;

b. Tracks users and intercepts their communications with healthcare-related websites, including the websites of medical providers subject to HIPAA; and

c. Takes and records users' medical communications and information for purposes of placing users into medical categories for direct marketing purposes in violation of Cal. Civ. Code §1798.91.

356. Facebook's conduct in tracking users and intercepting their communications with websites in violation of those websites' privacy policies is objectively unreasonable.

357. Facebook's conduct in tracking users and intercepting their communications with healthcare-related websites, including the websites of medical providers is objectively unreasonable.

358. Facebook's conduct in taking users' medical communications and information for purposes of placing them into medical categories for direct marketing purposes is objectively unreasonable as a matter of law because it is illegal under California law unless notice of the practice is provided in a clear-and-conspicuous manner and written consent is obtained from the person to whom the information is taken for direct marketing purposes.

359. Facebook's conduct in tracking and intercepting Plaintiffs' medical communications at issue in this case evades the spirit of the bargain made between Facebook and the plaintiffs.

360. Facebook's conduct in directly tracking and recording Plaintiffs' medical information to further Facebook's direct marketing purposes evades the spirit of the bargain made between Facebook and the Plaintiffs.

361. Facebook's conduct at issue in this case abuses its power to specify terms – in particular, Facebook's vague disclosures of its tracking which fail to disclose that it tracks and

intercepts communications in violation of other websites' privacy policies and tracks and intercepts communications with health-care related websites, including medical providers.

362. As a result of Facebook's conduct which is objectively unreasonable, evades the spirit of the bargain made between Facebook and its users, and abuses Facebook's power to specify terms in the contract it has with its users, Plaintiffs and the class members did not receive the benefit of the bargain for which they contracted and for which they paid valuable consideration in the form of their personal information which has ascertainable value to be proven at trial. Plaintiffs' actual and appreciable damages take the form of the value of their PII that Facebook wrongfully tracked and intercepted from their communications with health care websites and the medical information Facebook wrongfully used to place its users into medical categories for direct marketing purposes. In addition to these damages, Plaintiffs also seek nominal damages based on Facebook's breach of its duty of good faith and fair dealing, and disgorgement from Facebook of all the proceeds that it wrongfully obtained by breaching said duty.

COUNT IX – VIOLATION OF CAL. CIV. CODE §§ 1572 & 1573

(Against Facebook)

363. Plaintiffs hereby incorporate all other paragraphs as if fully stated herein.

364. Cal. Civ. Code § 1572 provides in relevant part that actual fraud exists when a party to a contract suppresses "that which is true, by one having knowledge or belief of the fact" "with the intent to deceive another party thereto, or to induce him to enter into the contract." In addition, it provides that actual fraud exists where there is "any other act fitted to deceive."

365. Cal. Civ. Code § 1573 provides in relevant part that constructive fraud exists "in any such act or omission as the law specially declares to be fraudulent, without respect to actual fraud."

366. Facebook violated § 1572, actual fraud, through its suppression, with the intent to deceive its users, of the facts that it (a) tracks and intercepts user communications in violation of other websites' privacy policies, (b) tracks and intercepts user communications with health-care related websites, including the websites of medical providers subject to HIPAA; and (c) tracks, takes, and records users' medical communications and information for purposes of placing users

into medical categories for direct marketing purposes. Plaintiffs relied on Facebook's false assertions in contracting with and using Facebook.

367. Additionally, Facebook violated § 1573, constructive fraud, by breaching its duty of good faith and fair dealing as alleged above and violating all of the assorted federal and state criminal and civil statutes alleged in this Complaint.

368. Plaintiffs, on behalf of themselves and the Class, seek damages from Facebook, including but not limited to disgorgement of all proceeds Facebook obtained from its unlawful business practices.

COUNT X – QUANTUM MERUIT

(Against Facebook)

369. Plaintiffs hereby incorporate all other paragraphs as if fully stated herein.

370. Facebook obtained a benefit from (a) tracking and intercepting user communications in violation of other websites' privacy policies, (b) tracking and intercepting user communications with health-care related websites, including the websites of medical providers subject to HIPAA; and (c), for Facebook, tracking, taking, and recording users' medical communications and information for purposes of placing users into medical categories for direct marketing purposes.

371. Facebook may not justly retain the benefit it accrued from (a) tracking and intercepting user communications in violation of other websites' privacy policies, (b) tracking and intercepting user communications with health-care related websites, including the websites of medical providers subject to HIPAA; and (c) tracking, taking, and recording users' medical communications and information for purposes of placing users into medical categories for direct marketing purposes.

372. Plaintiffs and the class members are entitled to restoration of their former position through compensation for the value of the sensitive personally-identifiable health-related information tracked and intercepted by Facebook without their knowledge or consent, and for disgorgement from Facebook of any proceeds that Facebook wrongfully obtained through its conduct.

VII. PRAYER FOR RELIEF

WHEREFORE, Plaintiffs respectfully request that this Court:

1. Certify this action as a class action pursuant to Rule 23 of the Federal Rules of Civil Procedure and appoint Plaintiffs as the representatives of the Class and their counsel as Class Counsel;

2. Award compensatory damages, including statutory damages where available, to Plaintiffs and the Class against Defendants for all damages sustained as a result of Defendants' wrongdoing, in an amount to be proven at trial, including interest thereon;

3. Award restitution to Plaintiffs and the Class against Defendants;

4. Award punitive damages in an amount that will deter Defendants and others from like conduct;

5. Permanently restrain Defendants, and their officers, agents, servants, employees, and attorneys, from disclosing, tracking, and intercepting the health-related Internet communications of Facebook users without consent or otherwise violating their policies with users;

6. Award Plaintiffs and the Class their reasonable costs and expenses incurred in this action, including counsel fees and expert fees;

7. Order that Defendants delete the data they collected about users through the unlawful means described above; and

8. Grant Plaintiffs such further relief as the Court deems appropriate.

DATED: March 15, 2016

KIESEL LAW LLP

By: /s/ Jeffrey A. Koncius
Paul R. Kiesel
Jeffrey A. Koncius
Nicole Ramirez

/ / /

/ / /

/ / /

THE GORNY LAW FIRM, LC
Stephen M. Gorny [to be admitted *Pro Hac Vice*]
steve@gornylawfirm.com
Chris Dandurand [to be admitted *Pro Hac Vice*]
chris@gornylawfirm.com
2 Emanuel Cleaver II Boulevard, Suite 410
Kansas City, MO 64112
Tel.: 816-756-5056
Fax: 816-756-5067

BARNES & ASSOCIATES
Jay Barnes [to be admitted *Pro Hac Vice*]
jaybarnes5@zoho.com
Rod Chapel [to be admitted *Pro Hac Vice*]
rod.chapel@gmail.com
219 East Dunklin Street, Suite A
Jefferson City, MO 65101
Tel.: 573-634-8884
Fax: 573-635-6291

EICHEN CRUTCHLOW ZASLOW & McELROY
Barry. R. Eichen [to be admitted *Pro Hac Vice*]
beichen@njadvocates.com
Evan J. Rosenberg [to be admitted *Pro Hac Vice*]
erosenberg@njadvocates.com
40 Ethel Road
Edison, NJ 08817
Tel.: 732-777-0100
Fax: 732-248-8273

THE SIMON LAW FIRM, P.C.
Amy Gunn [to be admitted *Pro Hac Vice*]
agunn@simonlawpc.com
800 Market St., Ste. 1700
St. Louis, MO 63101
Tel.: 314-241-2929
Fax: 314-241-2029

BERGMANIS LAW FIRM, L.L.C.
Andrew Lyskowski [to be admitted *Pro Hac Vice*]
alyskowski@ozarklawcenter.com
380 W. Hwy. 54, Ste. 201
Camdenton, MO 65020
Tel.: 573-346-2111
Fax: 573-346-5885

VIII. TRIAL BY JURY

Pursuant to the seventh amendment to the Constitution of the United States of America, Plaintiffs are entitled to, and demand, a trial by jury.

DATED: March 15, 2016

KIESEL LAW LLP

By: /s/ Jeffrey A. Koncius
Paul R. Kiesel
Jeffrey A. Koncius
Nicole Ramirez

THE GORNY LAW FIRM, LC
Stephen M. Gorny [to be admitted *Pro Hac Vice*]
steve@gornylawfirm.com
Chris Dandurand [to be admitted *Pro Hac Vice*]
chris@gornylawfirm.com
2 Emanuel Cleaver II Boulevard, Suite 410
Kansas City, MO 64112
Tel.: 816-756-5056
Fax: 816-756-5067

BARNES & ASSOCIATES
Jay Barnes [to be admitted *Pro Hac Vice*]
jaybarnes5@zoho.com
Rod Chapel [to be admitted *Pro Hac Vice*]
rod.chapel@gmail.com
219 East Dunklin Street, Suite A
Jefferson City, MO 65101
Tel.: 573-634-8884
Fax: 573-635-6291

EICHEN CRUTCHLOW ZASLOW & McELROY
Barry. R. Eichen [to be admitted *Pro Hac Vice*]
beichen@njadvocates.com
Evan J. Rosenberg [to be admitted *Pro Hac Vice*]
erosenberg@njadvocates.com
40 Ethel Road
Edison, NJ 08817
Tel.: 732-777-0100
Fax: 732-248-8273

THE SIMON LAW FIRM, P.C.

Amy Gunn [to be admitted *Pro Hac Vice*]
agunn@simonlawpc.com
800 Market St., Ste. 1700
St. Louis, MO 63101
Tel.: 314-241-2929
Fax: 314-241-2029

BERGMANIS LAW FIRM, L.L.C.

Andrew Lyskowski [to be admitted *Pro Hac Vice*]
alyskowski@ozarklawcenter.com
380 W. Hwy. 54, Ste. 201
Camdenton, MO 65020
Tel.: 573-346-2111
Fax: 573-346-5885